COVER STORY

The Fusion

Across the country, states and cities are finding new ways of sharing critical information.

By **PHILIP LEGGIERE**

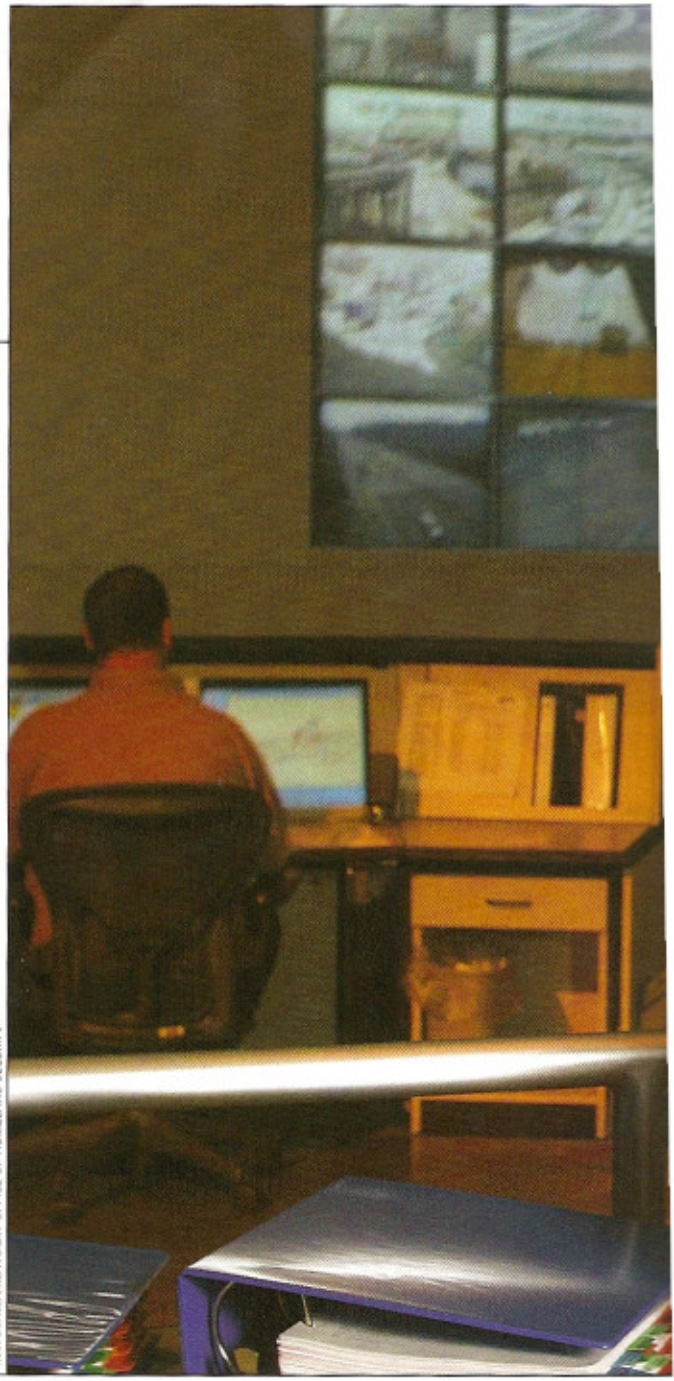
"OUR POLICE AGENCIES AND SHERIFF'S DEPARTMENTS ARE BLOODHOUNDS WITH THEIR NOSES TO THE GROUND. THEY HAVEN'T BEEN TRAINED, NOR DO THEY HAVE THE TIME, TO LOOK TO THE SIDE," REFLECTED RICH RAWLINS, DEPUTY DIRECTOR OF INTELLIGENCE AND THREAT ASSESSMENT FOR THE STATE OF OHIO.

Recent history, Rawlins acknowledged to *HSToday*, is tragically replete with examples of the limits of the bloodhound model. "The thing that every good law enforcement professional lives with every day now," Rawlins said, "is the knowledge that [his or her] most basic everyday investigations may intersect with a far wider universe of threats than most of us ever contemplated when we began our careers."

The example Rawlins referred to is that of Ziad Jarrah, the hijacker who piloted United Airlines Flight 93 on Sept. 11, 2001. On the night of Sept. 9, 2001, 48 hours before the takeoff of the infamous flight from Newark, NJ, Jarrah was stopped on I-95 by a state trooper in Maryland and given a speeding ticket.

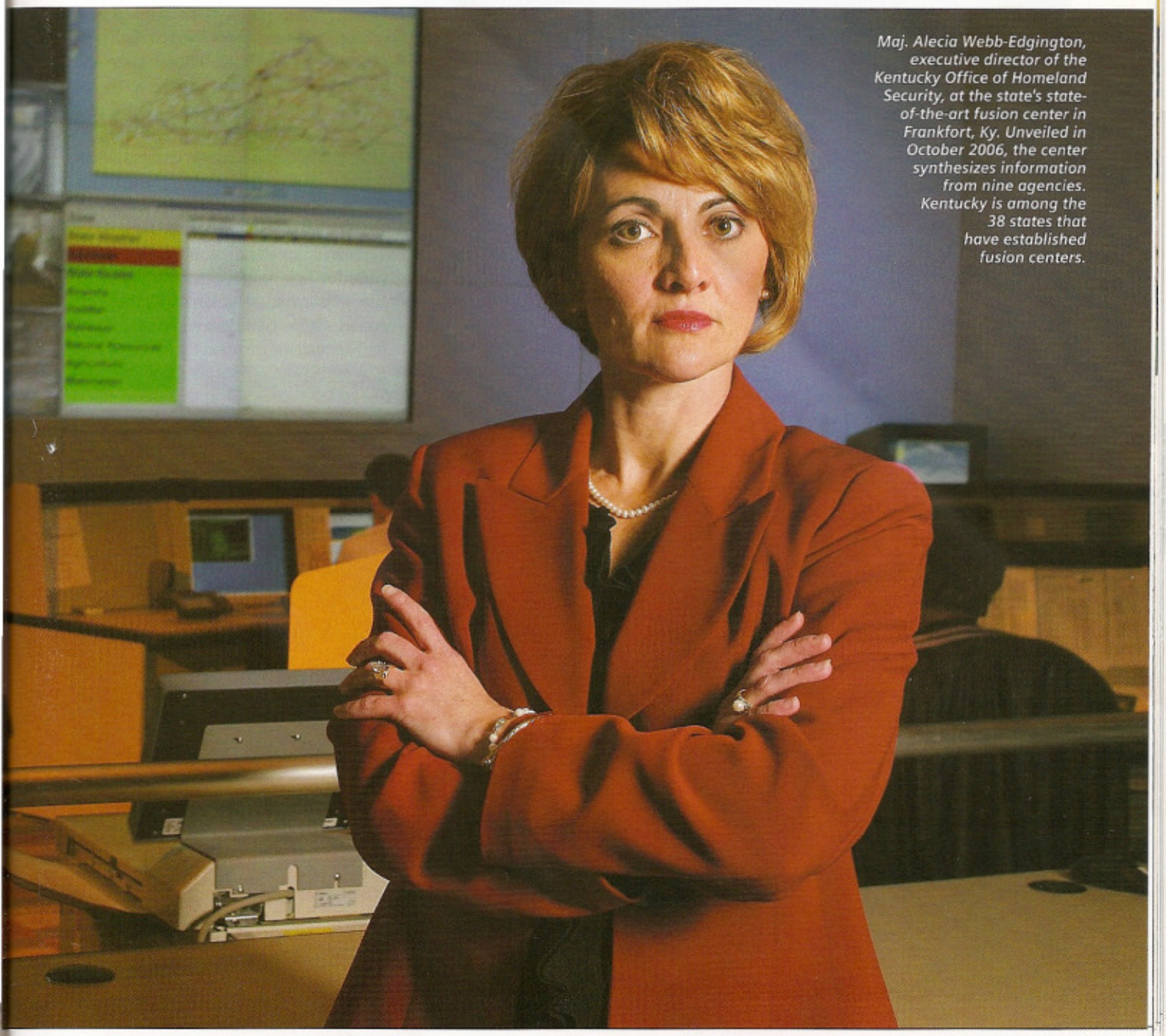
"Though there may in fact have been no way to make all the connections, you're haunted thinking that if only they'd been able to access the right piece of intel at the right time, information about what was being plotted may have been unraveled right there," he said. "But to make those kinds of connections, we have to move from just being bloodhounds on the track of the immediate threat and cultivate a kind of what you might call 'peripheral vision.'"

To cultivate that kind of "peripheral vision," more than three dozen states and cities across the United States have developed



KIRK SCHLEA/KENTUCKY OFFICE OF HOMELAND SECURITY

Revolution



Maj. Alecia Webb-Edgington, executive director of the Kentucky Office of Homeland Security, at the state's state-of-the-art fusion center in Frankfort, Ky. Unveiled in October 2006, the center synthesizes information from nine agencies. Kentucky is among the 38 states that have established fusion centers.

a new kind of combined law enforcement counterterror entity called the fusion center. Fusion centers are collaborative intelligence-sharing efforts between two or more agencies designed to pool resources on collecting, integrating and evaluating information of all kinds that may have a bearing on detecting criminal or terrorist-related activity.

"The premise and promise of the fusion center," said Chuck Dodson, senior director of justice and homeland security products at Redwood City, Calif.-based Oracle, "is to provide a way to enable law enforcement, public safety, emergency management and other partners to mutually aggregate, analyze and disseminate criminal and terrorist-related information." That promise has spurred a flurry of both federal initiatives and more locally generated projects over the past four years.

THE FEDERAL INITIATIVE

Since shortly after 9/11, the federal government has proclaimed the need to address the weaknesses in information sharing between agencies. This was frequently cited as a contributing cause of America's lack of preparedness for the hijackings. Two statutory mandates, the Homeland Security Act of 2002 and the Intelligence Reform and Terrorism Prevention Act of 2004, laid out ambitious directives for a unified national information sharing system.

The first bill requires presidential implementation of procedures under which federal agencies can share homeland security-related information with other federal agencies and with appropriate state and local personnel. The Intelligence Reform Act, passed in December 2004, requires presidential establishment and maintenance of an Information Sharing Environment (ISE) that will optimize policies and procedures to link people, systems and data, federal, state and local entities and the private sector. The act also requires the appointment of a program manager to oversee development of an Information Sharing Council (ISC).

Important steps toward uniform protocols and standards have been advanced. The Global Justice XML Data model is a data exchange standard that makes it possible for law enforcement agencies to share information without building new systems. An even wider-ranging standard, the National Information Exchange Model, is designed to extend the Global Justice model into other domains, including homeland security, immigration, intelligence and emergency management. Finally, a joint effort by the Department of Homeland Security (DHS) and Department of Justice has under development a National Information Sharing Strategy (NISS), a road map for seamless information sharing across agencies at all levels.

FROM THE GRASSROOTS

Despite these efforts and undeniable progress in getting funding from the federal to state and local level for data integration, the job of "standing up" operational data fusion is one that is primarily still evolving from the bottom up on a state by state basis.

"In practice the term 'fusion center' is a catch-all covering a variety of different initiatives," said Dodson. "Though their challenges ultimately may be the same, each state has a different mix of threats, resources, stakeholders, issues and skill sets. For that reason, important as federal leadership is, the fusion concept is being

largely created and sustained on a state and local level."

In January 2006 the Ohio Strategic Analysis and Information Center (SAIC) launched with over a half a million dollars in federal funding. The center, Rawlins said, is conceived less as a new centralized bureaucracy than as a nerve center bringing together agencies in addition to law enforcement to track and analyze trends from throughout the state that might relate to terrorist activity. These might include a pattern of theft of fertilizer or other potential explosive compounds, outbreaks of disease, mysterious deaths of fish in the state's waterways and many other scenarios.

Working as a partner with DHS, the center also exchanges data on a daily basis with DHS, and refers terrorist-specific "criminal intelligence" to five FBI Joint Terrorism task forces. Although the center only houses a dozen full-time personnel (who still draw salaries from their separate agencies), it acts as a crucial conduit of statewide information related to violent crime and potential crises. Among its ongoing responsibilities are collecting, collating, filtering, analyzing, disseminating and reviewing critical terrorist-related information from all sources; operating and responding to a toll-free telephone line; electronically filing, cataloging and cross-referencing sensitive intelligence bulletins, advisories and alerts to all sectors; maintaining a statewide situational awareness display at all times; and monitoring all evolving terrorist-related activities.

STATE EXPERIENCES

Although many states have established centralized fusion centers where multi-agency assets are brought together on a single location, Florida has opted for a slightly different approach it calls a "fusion process," in which information is shared and coordinated statewide through its Office of Strategic Intelligence via several cross-agency information sharing programs.

The Florida Department of Law Enforcement (FDLE) Counter-Terrorism Center collects and analyzes domestic security and terrorism-related information through a centralized statewide intelligence database called Threat.net, which is designed to allow federal, state and local agencies throughout the state to gather, analyze and share information about individuals and organizations involved in terrorism or terrorist-related activities.

FDLE also operates a statewide criminal justice network called CJNet that links all state and local databases relating to gang activity, drugs and suspicious activity. A recent FDLE initiative called the Critical Information Management System maintains real time displays on the status of Florida's critical infrastructure and can be accessed by the state's emergency operations center, all county emergency centers, all county sheriffs and county health departments, along with many local police, fire and EMS teams.

In Illinois, the concept of a fusion center, developed by the Illinois Statewide Intelligence Center of the Illinois State Police, has undergone several iterations over the past four years.

"When we started in 2003," recalled Col. Charles Brueggemann of the Illinois State Police, "we began as a terrorism information center where the object was to make terror database information accessible to officers in the field. As our information fusion efforts have evolved, we've moved toward an all-

Fusion solutions

Though the specific structure and state of the development of fusion center activities varies from state to state, there is a core of technologies and tools that law enforcement and other first response professionals currently have at their disposal to make cross-agency pooling and sharing of intelligence more viable. These include: data integration tools that tag and index data from disparate databases; collection tools that allow users to search for and access information across multiple databases; presentation tools that provide a unified interface through which data can be viewed; analytical tools that enable investigators to probe for significant links between data; reporting tools that allow information to be customized for specific contexts; and collaboration tools that enable sharing of documents, other data and applications.

To meet the needs of the centers, various technology vendors have made development of automated suites of these and related products a major priority.

"The proverbial task of investigators is to connect the dots, but before you can do that you need to be able to find the dots, and in an era of information overload, that's an overwhelming task. Analysts currently spend 80 percent of their time collecting data and 20 percent of their time making sense of it. The goal of technology developers is to reverse that proportion," said Rick McNees, vice president of business development at Chicago-based software firm River Glass Inc.

River Glass uses proprietary machine learning techniques that enable analysts at fusion centers to locate, analyze and act on both archived data from multiple sources and new incoming data. Teaming up with the Statewide Intelligence Center of the Illinois State Police, the company created a directory of definitions of over 85,000 key terms related to criminal and counterterror investigation scenarios.

This kind of directory, called an ontology, according to McNees, becomes a repository of expert knowledge through which search, analysis and reporting tools actually can progressively "learn" to map, model and present data with greater and greater precision and relevance to the specific needs of analysts.

"When you're searching huge volumes of data," McNees said, "relevance is the most critical thing. If you're compiling information about violent domestic organizations and just use Google, good as it is, it's not going to be able to distinguish that when you type in "ELF" you want to know about The Earth Liberation Front, not a Will Farrell movie."

Oracle's iHub addresses the task of integrating government data. The application suite, which combines Oracle's relational database and collaborative data integration software, allows states to create systems that can pull and display data from multiple databases, including any mix of federal, state, regional or local sources.

The Los Angeles County Sheriff's Department (LASD) is deploying a Web-based version of iHub to streamline investigative procedures across numerous law enforcement agencies

Continued on page 32

crime data fusion environment, and the next step is to move beyond that to encompass information on all hazards."

Working with the Chicago Police Department and statewide local police agencies, the Illinois State Police three years ago began developing ICLEAR, a statewide real-time data repository and warehouse of all-source information culled from over 1,200 law enforcement agency databases. Among the information shared on the system are terrorist threats, suspect lists, information related to gang activities, unsolved crimes and open arrest warrants. Also included are nicknames and aliases of known or suspected terrorists or criminal gang members, mug shots and other photos, vehicle information and miscellaneous data on suspects' tattoos, dress and other identifying features.

As the system has developed, Brueggemann said, the role of what's called "unstructured data" has become more important.

"There's an ever increasing universe of diverse information out there," he explained, "from videocams to sensors, [radio frequency identification] tags, instant messages, blogs and cell phone calls. It used to be that investigative databases were based primarily on what we'd call formal police records and documents. Those are still important, but they're just the tip of the iceberg of what needs to be integrated and looked at in analyzing trends."

Though fusion center managers acknowledge that the real benefits of data fusion and information sharing are more subtle and incremental than dramatic, all believe that even at this still early stage in deployment the new initiatives have improved practice.

"It may not be the stuff of [the television program] '24,'" said Rawlins, "but in emergency situations, the use of automated analytic systems can save lives that would have been lost before. Think about what happened to the 911 system during Katrina. You had thousands of calls—over 20,000 at one point—but no way to sort through all that overload of information, to analyze all that data and differentiate immediate life and death emergencies, like someone who needed his insulin shot in 30 minutes or he would die, from emergencies that could wait a little longer; and no way to get information to the [emergency medical services], fire and police officers at exactly the right place at the right time. The systems we're getting in place right now will make a big difference should an emergency of that magnitude hit our state."

Another benefit, according to Don Ladner, spokesperson for the Florida Office of Strategic Intelligence, is to enable analysts to separate out the noise and confusion that comes from emergency or simply panic situations.

"If there are 20 reports of sniper activity coming in from various sources simultaneously, you need to be able to figure out quickly how the accounts relate to one another and whether there's redundancy," said Ladner. "Is it 20 different snipers at 20 locations or one sniper that's being reported in 20 different versions? And if the latter, what's common and what's contradictory in those versions? This kind of thing can now be done in seconds."

The ability to relate seemingly marginal data points to other information in criminal suspect and unsolved case databases

is already proving itself in violent crime investigations. Using the ICLEAR database, police in a Chicago suburb were able to solve a home invasion and assault case by running the nickname of one of the perpetrators, overheard by the elderly victim in the crime, through the system. Using the nickname, police identified eight known criminals in the Chicago metro area. The victim recognized the mug shot of one, leading to the arrest and conviction of the offender—not only for the assault in question but also for several other local violent crimes.

The same technology is also being used, Brueggemann said, to pursue wider kinds of organized criminality. "Organized criminals, whether they're drug gangs or terrorists, all use the same state roads, bridges and other state services every day that law abiding citizens do," he pointed out. "They have houses and apartments, vehicles and even pets. They use computers and cell phones and go on social networks. There are networks of relationships and links that can be pieced together through all kinds of scattered reports. None of those things as isolated pieces of data necessarily mean much. But linked together they can generate connections that remained hidden before."

STOVEPIPES AND OBSTACLES

For all their promise, fusion centers face enormous hurdles in realizing their potential.

First, predictably enough, is resources. An estimated $380 million in funds from DHS have flowed into local, state and regional fusion center projects in the past five years, and federal funds were critical in standing up centers. The funding model to make them operationally sustainable on an ongoing basis remains to be worked out, however.

Second is training. Although technology vendors made important strides forward in making data integration and analysis applications intuitive and user-friendly, the fact remains that in the early phases of a fusion center, analysts with

Fusion Solutions

Continued from page 30

throughout the state. Using Oracle tools, the LASD interconnects over two dozen databases, allowing users throughout the system to instantaneously access background and historical information on criminal suspects.

"There are four key principles of [using computer statistics], said Dodson: "Timely, accurate intelligence; rapid deployment; effective tactics; and relentless follow-up and assessment. We believe the technology we've been advancing can help bring numbers one and four on that list up to speed for a new era where law enforcement and first response work is no longer confined to one city but needs to be informed by a far wider universe of data."

South Plainfield, NJ-based Instaknow's ACE is designed to run on top of existing database systems. The software's learning algorithm uses case examples to constantly refine and improve its information search and decision making capabilities. Once "trained," it can automate real-time interactions, streamlining data flow between the various internal systems of state agencies (for example, e-mails, instant messaging, word-processed documents), as well as external information such as Web searches and federal and national intelligence databases.

"In real world emergency management and law enforcement, situational awareness means retrieving and relating all sorts of disparate data in real time," said Paul Khandekar, chief executive of Instaknow. "There's no time for the kinds of executive decision support systems that work in business enterprises, but require extensive programming, data warehousing and replication."

Instaknow's tools are currently being used by Louisiana to integrate digitized information from police across the state, as well as fire and emergency medical services. The system's first applications are to provide unified, statewide, real-time information sharing on chemical spills and criminal background checks.

In dealing with a chemical spill, for instance, all state first responders will have access in real time to a common operating picture that seamlessly links them to National Institute of Science and Technology data on chemical properties, Google location maps, National Weather Service current wind and weather conditions, Federal Emergency Management Agency emergency contacts, Department of Transportation hazardous materials isolation guidelines and a National Response Center database of similar incident histories.

"In the past," said Louisiana State Police program manager Lt. Walter Wolfe, "responders and investigators had to access all of these different information sources as individual queries, leading to lost time, duplication of effort and the possibility, even the likelihood in an emergency situation, that crucial data sources will be overlooked."

Microsoft, Redmond, Wash., has developed a suite of applications to enhance integration, analysis and sharing of information for law enforcement and justice professionals. These include the Microsoft SQL integration and analysis server for centralizing data collection and management, BizTalk for XML-based information sharing, a Map Point system for geographic location visualization and three products, Groove, Live Meeting and Share Point for group collaboration. Using the Microsoft framework the state of Alabama developed a Law Enforcement Tactical System (LETS) to bring together cross-jurisdictional criminal justice data collected by agencies throughout the state. Law enforcement officers accessing the LETS Web portal can access millions of records, titles, photos and registrations updated in real time.

In addressing the fusion center market Microsoft, rather than merely selling off-the-shelf solutions, is committed to evolving a customizable architectural platform that is both scaleable nationally and adaptable to the unique conditions of each state, according to Joe Rozek, executive director of Homeland Security Intelligence and Information Sharing,

"Our goal," Rozek told *HSToday*, "is to be at the forefront of building a national information sharing environment from the ground up. Technology development approaches have to move beyond vendor-driven applications. Right now we're stepping back and listening to fusion center operators from all levels and asking the question: 'What is your vision? What processes are involved and how do you want to collaborate?'"

widely varying backgrounds come together. The need for uniform training methods and models becomes crucial.

"Simply having analysts from different agencies under one roof is not enough," argued Brueggemann. "Not if they're still tied to their old methods, procedures and skills. They not only need to be co-housed but co-mingled, and that's a function of training."

Third, the lack of consistent standardized policies and procedures remains a major gap. As the Markle Foundation National Task Force on National Security noted last year in its report, *Mobilizing Information to Prevent Terrorism* (http://www.markle.org/downloadable_assets/2006_nstf_report3.pdf), clear government guidelines for the handling of personally identifiable information have not been finalized.

Information sharing efforts also remain stymied by turf wars and unclear lines of control and responsibility. Despite the increased two-way flow of information between federal and state agencies, no consistent scheme of defining and relating different definitions of classified, sensitive-but-unclassified and unclassified information exists.

"Many of the stovepipes that stymied intelligence in the past are being overcome," said Dobson, "but the most deeply rooted stovepipe of all is that separating classified and unclassified data. They were designed so that never the twain may meet, but what we're learning is that, often, classified information held in federal databases may have no meaning unless related to a piece of unclassified data. So one important frontier of the near future is finding ways to securely relate the two sets of data while still maintaining access authorization control."

Nonetheless, signs of progress on these fronts are evident. "Two main things make me enthusiastic that the kinds of transformation we need to make data fusion and information sharing really work," noted Rawlins. "One is that, on the federal level, lots of smart people see the problems and are committed to really trying to tackle them with more than rhetoric. The other, and the most encouraging to me, is that whenever I talk to fusion centers in other areas, they are really excited to share advice and their experience in solving some of the problems we're working on. That tells me the culture of siloed information is definitely changing."

ANALYSIS

The shift from a traditional law enforcement and counterterrorism culture—in which information was collected and stored in siloed databases, hoarded territorially by agencies and distributed on a strict "need to know" basis—to one where "need to share" is the animating principle is one that will take not months or even years but decades.

At this point, useful guidelines are emerging at the federal level, and both states and technology developers are eager for more policy detail and clarity. Nonetheless, the transition is one that's being played out and taking root slowly, with lots of experimentation and trial and error, on a state-by-state basis. HST