Use of Technology in Intelligence Fusion Centers

An Oracle White Paper
April 2007

ORACLE

The Use of Technology in Fusion Centers

State and local law enforcement agencies are engaged in the day-to-day business of fighting crime and terrorism. A federal government, post event analysis concluded that sufficient information existed such that law enforcement officials could have intercepted the terrorists that flew aircraft into the World Trade Center. This “connecting-the-dots” philosophy relies heavily on real-time information integrated into a single comprehensive 360 view of the environment. The development and funding of intelligence fusion centers is a direct result of a need for better, more integrated information about suspects, locations, and conveyances that may be used in the planning or commission of a crime, including a terrorist act. The concept of the fusion center as an all source production of criminal and intelligence information is a good one. The weakness in the approach is the over reliance upon individuals staffing the fusion centers. In any business, labor costs are one of the biggest burdens to the profitability of the business. While current technology cannot replace the human brains ability for abstract thought and analysis, technology can provide methods and means for the collection, integration, analysis, and dissemination of all source intelligence to enhance fusion center operational efficiencies.

Introduction-

Developed in the aftermath of the September 11, 2001 terrorist attacks, the global Intelligence Working Group developed the National Criminal Intelligence Sharing plan. From this Plan, fusion centers were funded to support a formal intelligence sharing and communications structure.

“A fusion center is an effective and efficient mechanism to exchange information and intelligence, maximize resources, streamline operations, and improve the ability to fight crime and terrorism by analyzing data from a variety of sources.” (NCISP) As the fusion center model matures, it is becoming more integrated into a regional detect, deter, prevent, and respond model, integrating and sharing information with emergency management, firefighters, healthcare workers, etc. For the purposes of this paper we will focus upon primarily fusion centers and their law enforcement component.

Fusion centers provide all source collection and production of criminal and terrorism information from disparate individual or regional, state, local and federal databases. The end product of this all source production is to provide better situational awareness. The initial focus of the intelligence fusion center was to be the reduction of crime and the fear of crime. The desire for a fusion center with a multi-mission capability is illustrated by a quote from Los Angeles Police Chief William Bratton who said, “During World War II, we

fought on two fronts. We have to do this with terrorism and crime. We need to find a way to fight terrorism outside our country, prevent it inside our country, and to also deal with the problem of crime with its impact on human suffering". (PERF) In 2004, in support of this view, a new plan from the U.S. intelligence Czar proposed using fusion centers run by state police as hubs for counter terrorism intelligence and information sharing amongst state and local officials.

The 3-year plan for implementing the congressionally mandated Information Sharing Plan "provides a road map for the successful implementation of the ISE, and responds to the recommendations of the September 11 commission," said Thomas McNamara, program manager for the ISE in the Office of the Director of National Intelligence. Enacted as part of the 2004 intelligence reform law, ISE tried to create a seamless "network of networks" connecting officials -- and the terrorism-related information to which they have access -- by changing rules across the increasing number of federal, state and local agencies whose mission includes protecting the United States from terrorism. Mr. McNamara said the aim was to create "a virtual interstate system," and that the law-enforcement "fusion" centers being set up in states and large municipalities would be the "nodes where information can be processed, condensed and evaluated." (Waterman)

In the terrorism detect and deter mode, the fusion center may identify potential terrorist organizations, attack plans, funding sources, etc. In the prevention mode, the fusion center provides the ability for law enforcement to identify high value/risk targets and effectively deploy resources to them. Pre-incident planning, training, and exercises provide the foundation for the target analysis and vulnerability assessments. In the event of an incident, natural emergency or other crisis, the fusion center, depending upon the organizational structure and governance structure, can provide information to assist in the coordination and resource allocation of emergency operations centers, assist first responders and other tactical units, as well as identify additional emerging threats.

Fusion Centers

Most law enforcement agencies have a similar primary mission which may have been seen as a byline for one of the numerous police television dramas currently en vogue. The purpose of law enforcement is to protect and serve. Protect the lives and property of citizens and serve the community. The success of these missions is often evaluated by how well law enforcement reduces crime, and the fear of crime within their respective jurisdictions. After the terrorist attacks of September 11, 2001 the additional mission of detect, deter, and prevent acts of terrorism have been added to the services expected by governmental officials and the public.

Law enforcement and public safety agencies across the country today face substantial new challenges. One such challenge is to combat local and regional crime with diminishing resources and reduced budgets while, at the same time, remaining accountable for the reduction of crime and the safety of citizens.

Law enforcement and public safety agencies have encountered many disadvantages in this new mission tasking: agencies cannot securely share

criminal and terrorism intelligence regionally; track crime regionally and in real time; efficiently execute incident management; identify, quantify, assess, validate, manage, or provide analysis on a large number of critical infrastructure assets; and efficiently follow up to reduce crime, the fear of crime, and potential terrorist pre-incident and incident activities. Finally, almost all law enforcement agencies have a critical shortage of officers. It was in an effort to address these new challenges support for the development and funding of regional fusion centers has matured.

In the January 2006 issue of Police Chief Magazine, an article entitled "Intelligence Sharing: Efforts to Develop Fusion Center Intelligence Standards" outlines the basic foundations for the establishment of an intelligence fusion center. The Fusion Center Intelligence Standards Focus Group initially met in Atlanta, Georgia, on August 24 and 25, 2004, and again in January 2005. The focus group consists of representatives from a variety of local, state, and federal law enforcement agencies from across the country. The focus group participants have diverse experience and expertise; many members have been involved with developing fusion centers in their regions.

One of the first goals of the focus group was to develop guiding principles. These principles summarize the preliminary and overarching issues discussed by the focus group. They are provided as a guide for law enforcement agencies to use when establishing and operating intelligence functions within Fusion Centers. The guiding principles include the following:

- Adhere to the tenets contained in the National Criminal Intelligence Sharing Plan. The NCISP addresses a wide spectrum of intelligence issues and concerns. It provides model standards and policies and is the blueprint for establishing or enhancing intelligence functions.

- Collaboratively develop and embrace a mission statement-Mission statements provide focus and meaning for those participating in the fusion center. Mission statements should be clear and concise and should convey the purpose, priority, and role of the center.

- Create a representative governance structure- all participating agencies should have a voice in the establishment and operation of the fusion center and be adequately represented in the governance structure.

- Use a memorandum of understanding or other types of agreements as appropriate- Using a memorandum of understanding or other agreement defines the roles and responsibilities of the participating agencies.

- Integrate local, state, tribal, and federal law enforcement agencies- Fusion centers embody the concept of collaboration. Collaboration allows agencies to maximize available resources and work jointly toward a common goal.

- Create an environment in which participants can seamlessly communicate- Effective communications minimize the barriers that impede information sharing. Center personnel should strive to

ensure that information, whether electronic, verbal, or written, is accurate, complete, timely, and relevant.

- Develop, publish, and adhere to a policies and procedures manual- Policies and procedures outline the roles and responsibilities of the center. Policies and procedures ensure consistency, define accountability, reduce liability, and professionalize the overall operation.

- Develop, publish, and adhere to a privacy policy- it is critical that the civil and constitutional rights of citizens be upheld. Centers should develop, display, adhere to, and train personnel on the center's privacy policy.

- Ensure appropriate security measures are in place for the facility, data, and personnel- Security pertains to information, intelligence, documents, databases, facility, personnel, and dissemination. Centers should develop, publish, and adhere to a security policy and ensure proper safeguards are in place at all times.

- Integrate sworn and non-sworn personnel and ensure personnel are properly trained- People are the core of a successful fusion center. Ensuring a diverse workforce, with specialized knowledge and expertise, will create a trusted environment and will result in higher productivity and performance.

- Leverage existing systems and databases and allow for future connectivity- Centers should use resources already available, as opposed to creating new systems or databases. Centers should plan for future connectivity and adhere to standards. Participating agencies should use the latest version of the Global Justice Extensible Markup Language (XML) Data Dictionary when connecting databases or other resources to communication networks.

Operational Considerations

According to a survey conducted by the National Governor's Association in late 2005, the majority of fusion centers surveyed have many operational similarities. Most centers include staff from multiple agencies at the state, local, and federal levels and have established and maintain clear and direct communication channels to field officers and policy makers. Fusion centers are designed to be multi-purpose, focusing not only on terrorism prevention but also on fighting crime in general.

While there are similarities in operational configurations, variations also exist. Some fusion centers only have analytical roles while others also have the personnel and capabilities to act on intelligence. Some centers have a regional outlook, sharing information among states; others have a vertical structure, connecting states to local and federal agencies, but not to other states. While some fusion centers are contained within the federally led joint terrorism task forces, others are independent.

Typically, fusion centers consolidate resources from various participating

agencies into a single primary facility, with additional potential satellite locations. The intent of the co-location is to engender information sharing and rapid analysis by allowing access to multiple agency source systems in near real-time. Unfortunately, the solution has been to install standalone data terminals or computers and allow access only by that agency's onsite representative. One major challenge this configuration typically creates is the inabilities of the user [or agency] to collect, collate, analyze and distribute analysis across the region [enterprise is the term most often used by technical people]. These challenges can easily be overcome through the employment of modern, secure, and open architected information technologies. In reality, these technologies are often not deployed due to unyielding bureaucracies and outdated administrative policies.

Anticipated fusion center outputs are usually guided by the mission statement and operational focus. If the fusion center mission is oriented towards reducing crime and the fear of crime, then identifying crime trends and patterns to more effectively develop strategies and deploy resources in support of this mission becomes the expected outcome. If the fusion center also supports the identification, detection, deterrence, prevention, and the investigation of potential terrorist acts the products and outputs may be slightly different. Regardless, fusion center products will by necessity support these missions and will usually include administrative, tactical, strategic, and/or investigative analytical products.

Fusion centers offer a variety of intelligence services and must monitor outputs and outcomes to insure quality products and services to their consumers. Customers of the center expect timely and relevant intelligence services and products as well as investigative and tactical support. Centers should provide a variety of services and institute an evaluation process to ensure demands are met satisfactorily. By identifying appropriate and substantive performance metrics goals, expectations of local government, law enforcement executives, fusion-center personnel, consumers, and the general public can be clearly established. Quantitative measurement and evaluation of these performance metrics will identify the regional value added by the continued operation of the fusion center, and will be critical in securing additional funding.

Fusion centers encounter similar challenges that face law enforcement agencies, namely disparate data sources, resource constraints, increased operational expectations with reduced budgets, and a growing constituent expectation for greater accountability and transparency of operations. Fusion centers can address some of these challenges through leadership, improved training, clear and concise policies and procedures, and outreach towards the community. Other challenges can be met through an effective, strategic technology plan that leverages technology to provide more timely and actionable intelligence to focus deployed resources in an efficient and secure manner.

Fusion Center Technology

Technology should solve a business problem for the user. It is strongly encouraged that each fusion center have a strategic technology plan that identifies the business problems, potential technology solutions, and provides a roadmap for achieving the improvements necessary. While the use of

technology within the fusion center varies depending upon location, funding, technical expertise, and ability to support the technology purchased, this paper will focus on foundational information management technology and tools, and not niche commercial off-the-shelf vendor products.

In any discussion regarding the use and deployment of technology there is a zealous, almost a religious, argument over whether an agency should buy commercial solutions or build custom developed solutions. The basic questions as to buy-vs-build usually revolve around cost to purchase, implement, modify and maintain. Regardless of the decision to buy or build, the software solutions most commonly used within a fusion center will be either comprised of or built with database, middleware, integration, and business intelligence tools and products. Most products will utilize industry standard products, services, and processes so this is the area we are focusing on.

Justice Guidelines- The Justice Department released its first Fusion Center Guidelines making recommendations about the centers' law enforcement role, governance, connectivity standards, databases and security. "Related to IT needs, the report specifically recommends use of the Global Justice Extensible Markup Language (XML) data model, the Common Alerting Protocol messaging standards, and service-oriented architectures for improved information-sharing." (Washington Technology) While these technologies and standards will be addressed in more detail shortly, consideration should also be given to using data systems and architectures that are reliable, scalable, and provide adequate security and continuity of operations capabilities.

The Justice Department recommendations typically refer to the underlying foundation or architecture for an "Enterprise" regional information sharing structure. These recommendations help fusion centers collect, collate, and share information amongst disparate systems, for example sharing of information from numerous records management systems, computer aided dispatch, offender management, court, emergency management, and fire department operational systems. But technology can be employed to more efficiently provide analysis and dissemination of the volumes of data collected so that analysts and/or investigators can more quickly identify potential threats and conduct cursory or detailed investigations to confirm or dispel potential criminal and terrorist threats.

Fusion centers can leverage various other technologies to enhance operational efficiencies, improve information sharing and access to real time data to promote actionable intelligence sharing, focus deployed resources, provide timely information to first responders and ultimately safeguard our citizens and provide for more effective and efficient response. Some other technologies available include business intelligence, document management, identity management, search capabilities, and integration technologies.

Business Intelligence- Business Intelligence is also a technology layer within the fusion center architecture. This layer contains powerful services and applications that provide summary reports, ad hoc queries, geographic and geospatial queries, visualizations, OLAP, and data mining. This is the layer that provides users with intuitive tools to search, manage, and display information of interest. An example of business intelligence in a crime-

fighting context may be that a series of robberies occurs. By leveraging business intelligence tools, the analyst or investigator can quickly determine the locations of specific types of crimes, time of day/day of week parameters and identify common methods of operation and common suspect demographics to determine of there are any commonalities. This information can then be readily used to develop suppression or enforcement strategies to apprehend the suspect or suspects.

Document Management- Document Management provides complete lifecycle management of documents, enterprise sharing and audit/compliance requirements. Document Management for our purposes refers to the ability of the agency/user to secure, store, and share content efficiently. Investigative reports, incident reports, citizen tips, field interview cards, audio/video surveillance files, intelligence reports and bulletins are all examples of content that might be managed. Any enterprise quality solution should allow for offline editing/synchronization online. The benefit of document management is the speed and ability to quickly retrieve appropriate information for analysis or investigative purposes and then to share the documents and results across the enterprise.

Identity Management- most fusion centers have representatives from several agencies housed within a single building or location. The purpose of this co-location is to enhance information sharing in a timely fashion through access to multiple data sources in near real time. An unintended negative side effect is the management of user identifications and passwords. While it is probably not realistic to expect each of the legacy data source agencies to replace the security management infrastructure of all of their legacy systems, an agency can implement a single enterprise-wide solution for managing and authenticating users across the entire organization, including support for groups, roles, provisioning, audits, reports, etc., while protecting sensitive data.

This type of solution will help the organization achieve better security while reducing costs and risk. This capability provides the fusion center the ability to allow users access to multiple data systems without the need for those users to log in and out of each system, saving time and increasing user effectiveness.

Enterprise Search- One of the strengths of the fusion center is the amounts of data and resources available to focus on a particular problem or set of problems. The ability to conduct a search for structured and unstructured data is essential for the timely and efficient use of the information. Research conducted by Oracle Corporation has shown that most data within a system is about 80% unstructured data [text, spreadsheets, graphics, video/audio, etc] and 20% structured [structured data fields]; an enterprise search capability permits the user to search and retrieve information across the enterprise. The ability to leverage this massive storehouse of information is often dependent upon the users ability to quickly and easily search and retrieved critical information. If a person of interest is identified, an enterprise search would allow the user to search, retrieve, and display a consolidated view of that person quickly and easily.

Integration- The Fusion Center Guidelines suggest that the centers use a variety of databases, listing drivers' licenses, motor vehicle registrations,

criminal justice and corrections sources, and “public and private sources,” (Washington Technology) While this is a definite strength of the fusion center, it also adds a layer of complexity when attempting to integrate the data.

While discussing integration, there are several typologies, strategies, schemas, and other more technical terms to illustrate the details and complexities of data integration. For our purposes we will use patterns associated with Enterprise Application Integration, as explained in Wikipedia. Enterprise Application Integration typically refers to the integration of commercial off-the-shelf applications, as the name implies, but the basic concepts suffice for the purposes of this paper.

There are two patterns that Enterprise Application Integration systems implement: mediation and federation. In Mediation, the system acts as the go-between or broker between multiple applications. Whenever one of the applications is modified (new information created, new transaction completed, etc.) an integration module in the EAI system is notified. The module then propagates the changes to other relevant applications. An example of this approach that is commonly found in law enforcement integration systems is when a computer aided dispatch system creates or modifies information based on a call for service, this information is electronically provided to to the records management system to reduce duplicate data entry and auto-populate incident information. If the incident resulted in an arrest, the arrest information would be electronically provided to the jail management system, again reducing data entry, insuring data integrity and reliabilty, and improving operational efficiencies. The other pattern is a federated pattern.

In the case of a federated approach, the Enterprise Application Integration system acts as the overarching facade across multiple applications. All accesses from the “outside world' to any of the applications are front-ended by the Enterprise Application Integration system. The Enterprise Application Integration system is configured to expose only the relevant information and interfaces of the underlying applications to the outside world, and performs all interactions with the underlying applications on behalf of the requester. This approach is consistent with the concept of a federated query or search. That is I am looking for a suspect with a certain name and/or descriptor information. The Enterprise Application Integration permits the query and retrieval of all relevant information across the enterprise using the federated approach.

Both approaches are used within the fusion center, and law enforcement, environments, often concurrently. The strategy, approach, and methodology depends upon the source systems, the business problem being solved, and the architecture and expertise of the agency attempting to integrate.

There are other technologies such as data mining, spatial analysis, and others that can leverage or augment Business Intelligence, Document/Content Management, Identity Management, and Enterprise Search commercial products to solve specific business issues the identification of trends, patterns, and anomalous behavior.

Standards- Using industry acceptable standards are commonplace within the non-law enforcement community, as is the use of open architectures and

integrated systems that provide an enterprise view of all data. The use of business intelligence tools, data cleansing, and data-mining algorithms to enhance the quality and reliability of information are also common in the business world. In the law enforcement communities, the use of standards and information management tools/strategies is becoming more prevalent as these agencies recognize the cost savings and return on investment these approaches provide.

The information accessed, collected, analyzed and disseminated by fusion centers represents the gamut of sensitive information from nationally classified materials to law enforcement sensitive. Given that fusion centers all deal with sensitive information, the security requirements for their technology architecture are more stringent than for most commercial systems. A layered security model best addresses these requirements because a layered model has no single point of security failure.

Post September 11, 2001, the public sector has been mandated to transform itself from a “need to know” to a “need to share” community. Classified and sensitive information must be accessible, shared across networks and organizations, but still remain secure. Classified and sensitive information must be more accessible, shared across networks and organizations, but still remain secure. Fusion center solutions should focus on five problem areas for secure information sharing including cross-domain information sharing, cross-organization information sharing, cross organization information sharing, disconnected information sharing, and auditing.

Cross-domain information sharing is for the efficient management and sharing of data at different clearance levels across networks. Cross-organization information sharing provides for inter-agency, sensitive and/or classified data sharing across organizational domains. Disconnected information sharing addresses sharing of sensitive and/or classified data to disconnected devices, and auditing focuses on the centralized policy management and consolidation of audit records. Fusion centers may include several types of users, and any number of source data systems, including classified systems. To effectively leverage technology in a secure environment cross-domain, cross-organization, disconnected, and auditing concerns must be effectively addressed.

Global Justice Extensible Markup Language (XML)- “The Global JXDM is an XML standard designed specifically for criminal justice information exchanges, providing law enforcement, public safety agencies, prosecutors, public defenders, and the judicial branch with a tool to effectively share data and information in a timely manner. The Global JXDM removes the burden from agencies to independently create exchange standards, and because of its extensibility, there is more flexibility to deal with unique agency requirements and changes. Through the use of a common vocabulary that is understood system-to-system, Global JXDM enables access from multiple sources and reuse in multiple applications.” (DOJ-GJXDM)

“The Global JXDM was designed to provide XML components as building blocks for the schemas in Information Exchange Package Documentation (IEPD) IEPD's are baseline specifications that can be reused, extended, or adapted.” (DOJ-IEPD) The definition offered by the Department of Justice is “An “Information Exchange Package” represents a set of data that is

transmitted for a specific business purpose. It is the actual XML instance that delivers the payload or information"

The Global Justice Extensible Markup Language (XML) data model provides standardized information exchange protocol packages that enhance regional information sharing at a lower cost. This model has recently become the core foundation for the National Information Exchange Model. The National Information Exchange Model is designed to develop, disseminate and support enterprise-wide information exchange standards and processes. It originally was developed as an outgrowth of the Global Justice XML Data Model, but as it also matured data sharing protocols [Information Exchange Package Development] for fire, emergency operations, health, etc. It is hoped that the NIEM model will be adopted on an international scale.

Common Alerting Protocol - Common Alerting Protocol (CAP) is an XML-based data format for exchanging public warnings and emergencies between alerting technologies. Common Alerting Protocol allows a warning message to be consistently disseminated simultaneously over many warning systems to many applications. Common Alerting Protocol increases warning effectiveness and simplifies the task of activating a warning for responsible officials.

Individuals can receive standardized alerts from many sources and configure their applications to process and respond to the alerts as desired. Alerts from the United States Geological Survey, the Department of Homeland Security, and NOAA can all be received in the same format, by the same application. That application can, for example, sound different alarms based on the information received.

By normalizing alert data across threats, jurisdictions and warning systems, Common Alerting Protocol also can be used to detect trends and patterns in warning activity, such as trends that might indicate an undetected hazard or hostile act. From a procedural perspective, Common Alerting Protocol reinforces a research-based template for effective warning message content and structure.

The Common Alerting Protocol data structure are backward-compatible with existing alert formats including the Specific Area Message Encoding (SAME) used in Weatheradio and the broadcast Emergency Alert System, while adding capabilities including: Flexible geographic targeting using latitude/longitude "boxes" and other geospatial representations in three dimensions; Multilingual and multi-audience messaging; Phased and delayed effective times and expirations; Enhanced message update and cancellation features; Template support for framing complete and effective warning messages; Digital encryption and signature capability; and, Facility for digital images, audio and video.

Services Oriented Architecture- "A paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with and use capabilities to produce desired effects consistent with measurable preconditions and expectations." (Wikipedia-SOA)

One of the recommended methods for using disparate databases is through

Services Oriented Architectures. Today's applications are evolving from being monolithic, closed systems to being modular, open systems with well-defined interfaces. This new application architecture, called service oriented architecture (SOA), represents a fundamental shift in a way new applications are being designed and developed, and the way they are being integrated with the existing legacy systems.

A service-oriented architecture provides a standards-based platform that allows services to be provided, discovered, and consumed by each other, to facilitate the creation of a business process. SOA requires several pieces of basic functionality to operate correctly and provide the most value. Here are the necessary components of a service-oriented architecture:

- Leverage of existing investments. For SOA to offer value, it must leverage existing systems. Service-enabling existing systems increase the usefulness and value of those systems. Suddenly, existing systems can be used in new ways and pressures to update those systems decrease.

- Loose coupling. SOA embodies the concept of loose coupling. When the interface is abstracted out, changes in one system do not affect others. This reduces the cost of change, by eliminating the need for extensive retesting if one minor change is made within one system. Because the systems are not directly dependent on each other, changes in one system are not likely to percolate to another system.

- Service encapsulation. Encapsulation separates the interface from the way the service is performed. This enables the underlying implementation of the service to change without affecting the integration. This reduces the risk associated with future platform changes.

- Interface standardization. Using standards when developing interfaces lets the interfaces interoperate more easily. Web services standards such as Simple Object Access Protocol (SOAP) and Web Service Description Language (WSDL) enable heterogeneous systems to interoperate.

- Shared semantic framework. Semantics are the vocabulary of any service; utilizing the same semantic framework enables various systems to understand each other. With a shared vocabulary, or semantic framework, those systems can more easily communicate. This shared semantic framework can consist of the same definition structure or the ability for a term to be translated into a common definition.

- Business events. A business event is a state-change notification that requires human or system intervention. The event moves the business process along, either starting it or providing a key component within it.

As you can see, the United States Department of Justice provided a good set of recommendations for the foundation of information sharing within the

law enforcement community, and specifically fusion centers. Although these recommendations were a good beginning, there are several technologies and tools that can be leveraged to enhance the ability of fusion centers to accomplish their respective missions.

Conclusion

Most law enforcement agencies have had a similar primary mission; that is to serve and protect the citizens and property within their respective jurisdictions. As a result of the terrorist attacks of September 11, 2001 the law enforcement community gained the additional mission of detection, deterrence, and prevention of future terrorist attacks. As a result, the law enforcement community must not only deal with the day-to-day issues of crime and the fear of crime, but also the once in a career terrorist attack.

Fusion centers were developed as a response to the terrorist events that occurred on September 11, 2001. The concept of regional information sharing to fight crime was expanded to include the evolving law enforcement role of detection, deterrence, and protection against terrorist acts.

There are similarities and disparities within the various fusion centers. Some fusion centers have only analytical roles while others also have the personnel and capabilities to act on intelligence and conduct investigations. Some centers have a regional outlook, sharing information among states; others have a vertical structure, connecting states to local and federal agencies, but not to other states. While some fusion centers are contained within the federally led joint terrorism task forces, others are independent. Regardless of these similarities and disparities, each fusion center has a shortage of resources, budget, and personnel to address all contingencies. By leveraging technology, fusion centers maybe able to mitigate the impact of some of these challenges.

The United States Justice Department has provided fusion center guidance and has encouraged the use of industry standards such as Global Justice XML Data Model and the National Information Exchange Model. The government has also supported Services Oriented Architecture for use within fusion centers. There are, however, a number of industries standard technologies not mentioned by the government, even though they are in use by law enforcement agencies and commercial businesses alike. The use of business intelligence, document and identity management, enterprise search, and integration technologies can all enhance the capabilities and effectiveness of fusion center analysts, administrators, and investigators.

Technology offers the potential for fusion centers to enhance analysis and dissemination of timely and accurate actionable intelligence in near real-time. By leveraging technology fusion center administrators can enhance the efficiencies of their participating analysts and investigators, while enhancing and promoting greater visibility and transparency of government. While all of the above benefits are significant and important, the effective use of technology can help law enforcement “connect the dots” to prevent another act of terrorism, thereby saving lives.

References

Institute for Intergovernmental Research, *National Criminal Intelligence Sharing Plan,* 2005, downloaded from the World Wide Web on December 5, 2006 from www.iir.com/global/ncisp.htm

Waterman, Shaun, *State police eyed as hubs of terrorism data network*, United Press International, November 24, 2006

National Governor's Association, *State Intelligence Fusion Centers: Recent State Actions,* 9/19/2005, downloaded from the World Wide Web on December 5, 2006 from http://www.nga.org/portal/site/nga/menuitem.9123e83a1f6786440ddcbeeb501010a0/?vgnextoid=7d7e37a59b066010VgnVCM1000001a01010aRCRD

Alice Lipowicz, *Justice issues fusion center guidelines*, Washington Technology 8/30/05, downloaded from the World Wide Web on December 5, 2006 from http://www.washingtontechnology.com/news/1_1/daily_news/26893-1.html

Wikipedia, *Common Alerting Protocols*, downloaded from the World Wide Web on December 5, 2006 from http://en.wikipedia.org/wiki/Common_Alerting_Protocol

Wikipedia, *Service Oriented Architecture*, downloaded from the World Wide Web on December 5, 2006 from http://en.wikipedia.org/wiki/Service-oriented_architecture

Oracle Corporation, *Services Oriented Architecture* White Paper, downloaded from the World Wide Web on December 5, 2006 from www.oracle.com

Dodson, Chuck, *Fusion Center Use of Technology*, All Hazards Forum presentation dated October, 2006, downloaded from the World Wide Web on December 5, 2006 from www.allhazardsforum.com/speakerpresentations/october11/Dodson.pdf

Police Chief Magazine, "Intelligence Sharing: Efforts to Develop Fusion Center Intelligence Standards", January 2006.

U.S. Department of Justice, *Information technology Initiatives*, downloaded from the World Wide Web on December 5, 2006 from http://www.it.ojp.gov/jxdm/

Police Executive Research Forum, *A Gathering Storm - Violent Crimes in America*, October 2006

Intelligence Fusion Centers
April 2007
Author: Chuck Dodson
Contributing Authors:

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
www.oracle.com