

WHITE PAPER

First Responders and Beyond: How Data Integration Enables Homeland Security

Sponsored by: Oracle

Shawn P. McCarthy
May 2004

Introduction

After a period of stagnation, government spending on information technology products and services is steadily improving. The catalysts are homeland security and a series of grants from the Department of Homeland Security (DHS) directly to states (nearly \$8 billion in the past 16 months). In many cases, these grants have targeted first responder efforts. Data sharing between agencies and emergency access to information are primary goals.

Most state and local IT managers have had to do more with less in recent years. In 2003, 27 states suffered significant budget gaps, according to the National Conference of State Legislatures. Many IT departments saw no budget growth at all. New homeland security money is welcome but may not address pressing IT needs.

Two needs, outlined in a recent IDC survey of state and local IT managers, are the desire to adopt an enterprise view of government services and the ability to facilitate interagency communications. It is fortuitous that homeland security needs actually dovetail with these state and local needs. State and local governments likely will spend some homeland security money on systems that serve dual or multiple uses as well as help them meet their ongoing IT challenges. At the state and local levels, IT managers find themselves working closely with police chiefs, fire chiefs, public health officials, and others who have a need for first responder systems.

The president's national strategy for homeland security includes the following objectives: "Prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recovery from attacks that do occur." The strategy requires previously separate agencies to "focus and integrate our collective efforts" on solving homeland security issues. In short, this means intensive data sharing and analysis, which can be targeted at short-term emergencies such as responding to an attack or national disaster or at ongoing issues such as monitoring suspicious people or activities.

Homeland security efforts require considerable investments in security screening, data gathering, and integration (for the merging of data and systems) and analysis technologies. The objectives of these investments are to improve information access and identify potential threats. Key technologies include sensors and surveillance equipment, wireless and handheld mobile devices, biometrics, databases, network infrastructure, and new applications and Web services focused on integrating existing data sources and systems. Geographic information systems (GIS) that integrate multiple data sources and display the data as map overlays are a popular solution, particularly for justice and public safety organizations.

In This White Paper

This white paper focuses on the provision and integration of information to support homeland security efforts, particularly for first responder (justice and public safety) and public health communities. The document explores Oracle's solutions to these challenges, based on briefings by Oracle's homeland security team, interviews with Oracle's homeland security partners, and interviews with customers that have implemented Oracle solutions to enable first responders. The paper:

- ☒ Presents the needs and challenges of first responders, primarily justice and public safety and public health workers
- ☒ Profiles Oracle's approach to delivering homeland security solutions to support first responders and public health organizations, including its iHub solution
- ☒ Discusses Oracle's partners strategy and profiles three of Oracle's key partners — PlanGraphics, SRD, and Ship Analytics — in delivering homeland security solutions
- ☒ Concludes with a case study of how Oracle worked with the New Jersey Office of Emergency Management to develop a first responder system

The First Responder Need

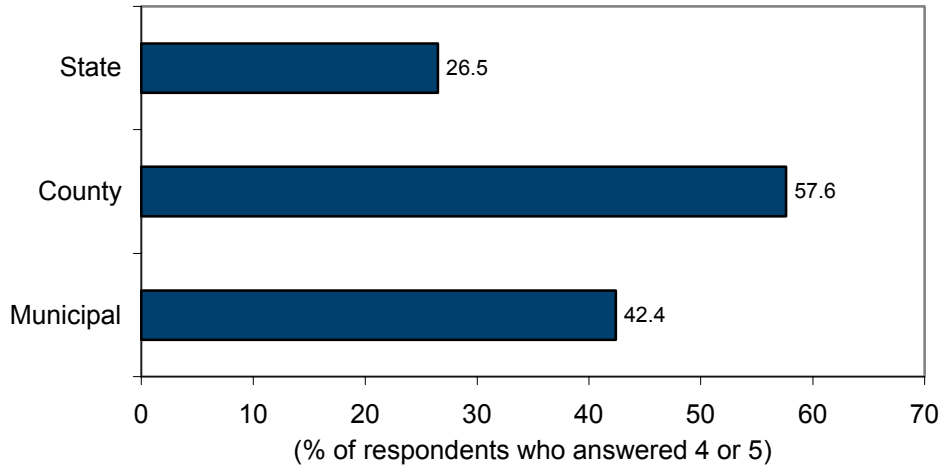
IDC has observed two overarching homeland security themes from discussions with government officials. The first is the desire for secure data sharing and integration between agencies. The second is meeting the information needs of first responders. Because local governments face multiple challenges, homeland security as a standalone concept has been on their radar screens, but it is not currently a top priority. Figure 1 reflects this ambiguity. IDC sees a broad opportunity for vendors that have the ability to implement systems that "kill two birds with one stone." These solutions can improve data sharing between agencies while also streamlining ongoing business processes — both of which can greatly benefit justice and public safety and public health workers on a daily basis as well as help prepare them for emergencies.

Figure 2 shows that the focus on IT as a primary solution to these problems seems to be greater at the state level than the local level. The latest round of state grants from DHS reinforces this orientation, as municipalities wait for monies to trickle down before committing homeland security funds to major IT projects.

FIGURE 1

Homeland Security Solutions Are Important to Local Governments

Q. On a scale of 1–5 (with 1 being not important and 5 being very important), please rate how important implementing homeland security is to your agency's FY 2004 strategic priorities.



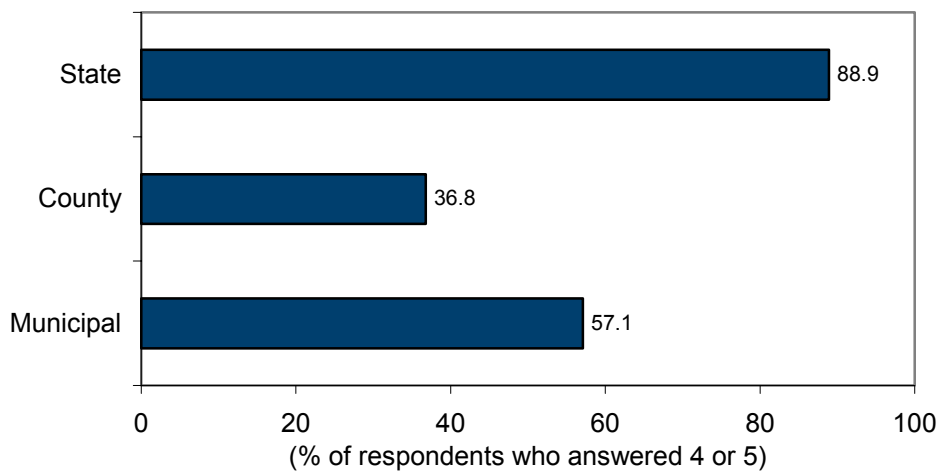
n = 100 respondents who work for state or local government IT offices

Source: IDC's *State & Local Government Survey, 2004*

FIGURE 2

Importance of IT to Homeland Security

Q. On a scale of 1–5 (with 1 being not important and 5 being very important), please rate to what extent IT will have a role in addressing challenges of implementing homeland security.



n = 42

Source: IDC's *State & Local Government Survey, 2004*

Justice and Public Safety Officials Benefit Daily from First Responder Systems

There is an ongoing homeland security challenge for federal, state, and local governments. This challenge is to enable interaction between law enforcement, public safety, and public health officials at all levels of the government and to develop timely, actionable, and valuable information through intensive data sharing.

The objective of developing powerful homeland security–focused first responder systems for justice and public safety officials is not exclusive of the ongoing goals of state and local governments to improve workflow and service to citizens. The most useful first responder solutions will be crafted with other day-to-day uses in mind. Being able to meet the multiple needs of justice and public safety workers provides greater value and greater return on investment (ROI) to government agencies. These needs include:

- ☒ **Availability of information.** In times of emergency, two important issues for homeland security are quick network access and the availability of appropriate information to first responders. The first officials to arrive on the scene of any emergency, or the first people to encounter suspicious activity while doing their jobs, need real-time access to multiple types of government data — personnel, maps, and equipment. Most important, they need access to information about local resources, including law enforcement, fire departments, public works contacts, ambulance services, intensive care facilities, rescue equipment, and public health organizations.
- ☒ **Data integration.** Cross-agency cooperation for information sharing and integration of multiple data sources is necessary to support the efforts of first responders. This cooperation is not easy to achieve because databases have different data fields, naming conventions, and access controls. Likewise, key resources may be available from the private sector, but if data about those resources is not easily available to first responders, then they may not be able to call on these additional assets. What is needed is a system that merges this data in an understandable way.
- ☒ **Security.** Across the different homeland security initiatives, IDC research has found that government organizations have spent an average of half of additional homeland security funds on IT security technologies such as antivirus tools and firewall appliances. Current adoption of technologies such as smart cards, profiling tools, and biometrics is a bit slower because these technologies are in the emerging stages, and many government agencies are just beginning to understand how these types of technologies can be applied to their situation. It is important to point out that specific technologies, such as biometrics and profiling tools, may be best suited for specific functions, such as public safety.
- ☒ **Mobility.** Mobile enterprise applications for government employees — and emergency responders — are of growing importance. The state of Texas has deployed mobile applications to more than 250 government inspectors who license and inspect more than 23,000 childcare facilities through the Texas Department of Protective and Regulatory Services. By replacing the original manual, paper-based system, these applications enable inspectors, via handheld devices, to capture pertinent information and transmit inspection reports while in the field. Mobile enterprise applications can easily be adapted for data collection in emergency situations.

- ☒ **Need to share.** Traditionally, government communicates information on a "need to know" basis, but public safety information often requires a "need to share" approach. This means that first responders may not know what is available to them, while those who have equipment, services, and labor resources need a way to announce their availability. Need to share is a much different paradigm for most government organizations. Few municipalities have systems in place to enable the need to share model, but constructing such systems is not complex if the right tools and technologies are used.

Data Integration Helps Public Health Organizations Respond to Homeland Security Incidents

A key driver of IT and homeland security investment in governments and public health organizations is the leveraging of technology to develop new ways to share data across agencies and government offices. As government agencies and public health officials find an increasing need to share information — particularly as they face the daunting task of protecting the country from foreign and domestic terrorism — they are turning to new database solutions and application development tools to address their data sharing needs. Public health systems can further benefit from integrated data sources to better respond to bioterrorism incidents and other health emergencies. For example:

- ☒ A GIS system, placed online or within kiosks, can provide interactive information to support public health strategy and education. The U.S. Centers for Disease Control and Prevention's Injury Center adopted mapping technology to create an interactive Web-based mapping application displaying levels of injury-related mortality in the United States, including specific regional patterns.
- ☒ Another example is that healthcare research professionals can use the tool to create regional maps illustrating illness patterns and virus movement. This information can be used by government agencies, health departments, and policy makers to make decisions and support public health education initiatives.

Oracle's Homeland Security Solutions

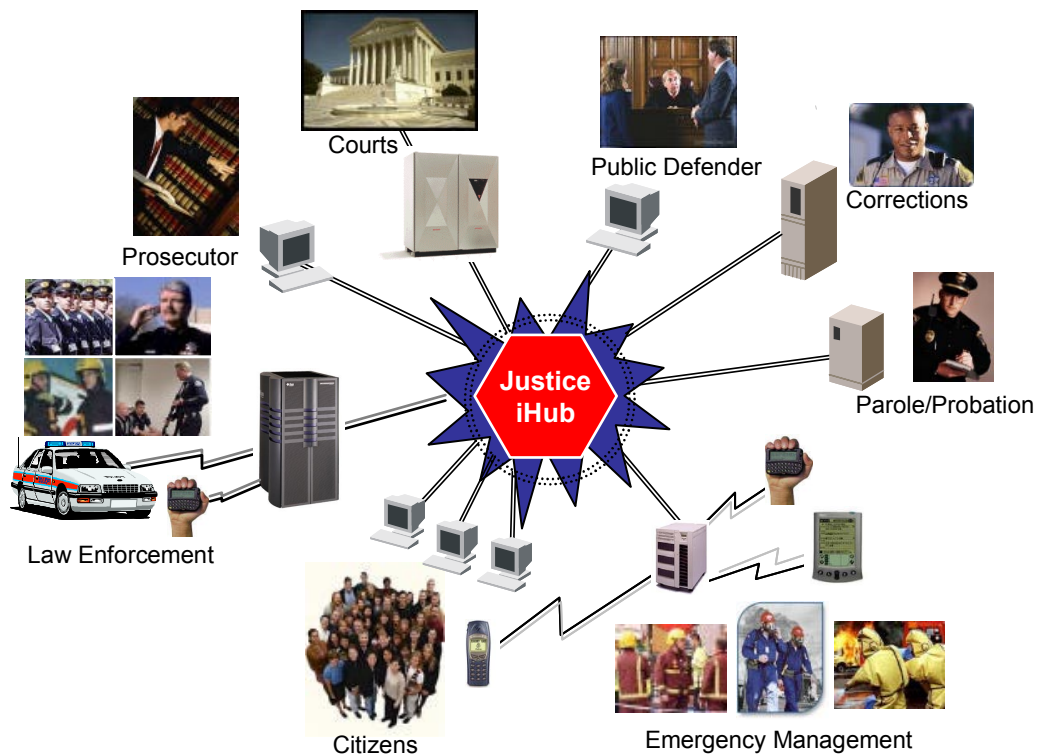
Government agencies and public health systems of all sizes need help with the complex task of integrating data from multiple sources and building easy-to-understand interfaces to first responder systems. More than 2,000 government agencies worldwide rely on Oracle's information management and expertise, and over 100,000 professionals in DHS use Oracle to support their daily missions. Also, Oracle has a history of developing intelligence-related applications. The Central Intelligence Agency (CIA) was one of Oracle's first customers back in the 1970s, and Oracle's databases and technology are now used by the CIA, the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) for many robust and mission-critical needs.

Oracle's iHub is a solution that is specifically designed for integrating government data and building new shared applications to display that data — specifically addressing homeland security pain points at the federal, state, and local levels. One example is the Oracle Justice Integration Hub (Justice iHub). The Justice iHub is the platform that can reside at any jurisdiction to service a single agency or multiple

agencies and their justice trading partners (see Figure 3). Authorized users can access information through a role-based Justice Enterprise Portal. Users can push, pull, publish, subscribe, or query data across an enterprise of disparate databases. This eliminates redundant data entry and improves the quality and integrity of the criminal history record. Offenders can be identified more quickly when stopped by the police, and justice can prevail more regularly when sentences are decided based upon better, more readily accessible information.

FIGURE 3

Oracle's Justice iHub



Source: IDC, 2004

For other iHub solutions, information can be extracted into a data warehouse for tasks such as investigative analysis or crime analysis. Information collected from the source systems may provide the data to be displayed in "real time" and analyzed in preparation for, during, and after law enforcement operational reviews, often referred to as COMPSTAT (Computational Statistics). Hours of pouring through reports and paperwork to prepare for COMPSTAT will be replaced by logging onto the system and getting up-to-the-minute statistics with the ability to drill-down for further information; for example, for a specific precinct, type of crime, or time duration. By incorporating geospatial analysis into the solution, government agencies can use visual pattern analysis for further crime-fighting techniques.

Oracle also has a series of products that can be used in concert to build integrated systems capable of pulling and displaying data from multiple sources. The information then can be made available to first responders and other government agencies. In some cases, this information can be provided via single sign-on systems developed specifically for incident management.

The foundations of such a system are the construction of a trusted information grid with the potential to encompass data from international, federal, state, and local government sources and the ability to publish and subscribe data in a secure manner between networks of different levels of classification. If needed, commercial data sources and records also can be integrated. Such systems are beyond the capabilities of current commercial off-the-shelf (COTS) solutions. They need to be highly customized because data sources and security levels vary greatly from one municipality to the next. Most systems will be built using a combination of direct log-in to relevant systems plus extensive Web services that work in the background to authorize secure data access and import from additional systems.

The effort to build integrated dual-use systems that can be used in the office or in the field comes at a good time. By the end of 2004, network access will be made easier for first responders with the advent of city-wide Wi-Max systems. Wi-Max is the nickname given to the Institute of Electrical and Electronics Engineers (IEEE) 802.16 standard and other wireless specifications that allow network connectivity over distances of up to 30 miles. Thus, first responders with properly enabled laptops will be able to access the Internet, government networks, and relevant online resources from their vehicles — anywhere in a metropolitan area that is equipped with Wi-Max transceivers.

Whether access is gained through Wi-Max or more traditional network access points such as DSL line or satellite uplink, the system concept is the same. The foundation is a technology platform — in this case Oracle's — plus multiple data sets and a suite of tools and easy-to-understand interfaces designed to help teams administer intelligent and coordinated responses during an emergency.

Oracle products are currently used for mission-critical systems by DHS and state and local governments. These include systems at the Federal Emergency Management Agency (FEMA), the FBI's National Infrastructure Protection Center, and dozens of other agencies. Oracle has become one of the most common database and application development environments in use today in government offices. Oracle also has built-in security and access controls.

In addition to general database access and search tools, two special applications that first responders should find useful are the Oracle inventory tracking and supply chain management technologies used by manufacturers and retailers. When applied to a first responder system, these tools can be used to show everything from available emergency equipment and medical supplies to available hospital beds in the surrounding area to details from police bulletins.

Oracle's Product Suite: The Foundation for Homeland Security Solutions

Oracle occupies a unique market space in that it offers database tools, application development tools, and a suite of existing applications that integrate and extend a variety of business functions. The basic lineup of products is as follows.

- ☒ **Database.** The foundation of Oracle's product line is its powerful and secure database, currently known as Oracle Database *10g*. It is specifically designed for grid computing and has a variety of price points, depending on the size of the installation.
- ☒ **Oracle Application Server.** This offering includes the tools needed to develop, integrate and deploy ebusiness portals, transactional applications, and secure Web services.
- ☒ **Oracle Applications.** This complete set of business applications enables organizations to manage and automate companywide processes and can be used out of the box or customized depending on local needs.
- ☒ **Oracle Development Tools.** The tool set offers an integrated environment that combines application development and business intelligence tools.
- ☒ **Oracle Enterprise Manager.** This single, integrated product monitors and manages an Oracle software infrastructure as well as applications and business services in diverse IT environments.
- ☒ **Oracle Collaboration Suite.** The suite provides an integrated system for an organization's communications and information needs, including Web conferencing, file sharing, email, messaging, voicemail, fax, and wireless.
- ☒ **Oracle Services.** In addition to databases, applications, programming, engineering tools, and systems integration services, Oracle provides special consulting, application development, and training.

Special Products for First Responder Systems

For most installations, Oracle uses as much of its own technology as possible. But Oracle also works to pursue close integration with complementary third-party technologies when appropriate. The following Oracle products are potential add-ons for first responder systems:

- ☒ **Alerting and notification** sends secure alerts to other users based on geographic location and user profile. These alerts can be actionable, provide feedback to the sender, are easily customizable, and support a large number of devices.
- ☒ **Emergency multichannel messaging** notifies all users as new information or orders become available and sends links or attachments as needed.

- ☒ **Knowledge management and distance learning applications** can be used to train emergency personnel while they are on site, giving them access to relevant information, such as hazardous materials databases or evacuation routes.
- ☒ **Oracle Threat Manager** integrates information about assets, reported threats, types of targets, and ongoing responses, providing a visual dashboard of what is being investigated and protected.

Oracle's Homeland Security Partner Strategy

With a significant government presence, Oracle is already heavily involved in homeland security efforts. When focusing on providing solutions to the first responder and public health communities, Oracle provides a secure foundation, database, development tools, and application environment. Because homeland security is a mission-critical process that cannot be supported by a single, specific product, Oracle's homeland security strategy is to go to market with partners that offer targeted solutions to address key operational requirements. Concentrating on the strengths of this ecosystem of partners has led to a number of prepackaged homeland security solutions that are being successfully used today.

Oracle began its homeland security partner program in January 2002. It currently partners with more than 150 companies and works most closely with a core group of 50 to 60 partners. This group has evolved into a cooperative community of partners that work closely together and develop new ideas and create and test cross-functional products. Solutions may include a number of the following key requirements in order to address homeland security needs:

- ☒ **Biometrics and identity management**, including fingerprints, iris scans, and facial recognition systems, are key components being used for physical access to facilities, access to IT systems and applications, and authentication of identity. Biometrics also will be incorporated into passports starting in October.
- ☒ **Incident management/command and control** applications that help streamline the process of dealing with a disaster or emergency situation are needed by first responders and other public service organizations. This type of application can also be applied to limited time events, such as security needs during music festivals, conventions, or the Olympics.
- ☒ **Document authentication and version control** for application development management, content management, and compliance.
- ☒ **Radio frequency identification (RFID) and sensor-based computing** uses everything from inventory tracking and cargo security to monitoring ambient levels for pollutants or toxins in the environment.
- ☒ **Critical infrastructure protection** focuses on securing everything from data, machines, and networks to physical plants. These solutions work to ensure constant operation, capacity, and resiliency in mission-critical systems.

- ☒ **"Spatially enabling" the enterprise** provides geographic reference information to existing data, which then allows location to be used to provide relevant related information. For example, a hospital system can track assets, skill sets of personnel, and local transportation data, all of which can be used for contingency planning in case of inclement weather or mass casualty traumas.
- ☒ **Turning data into actionable intelligence** by integrating multiple sources of information, resolving ambiguities, and providing a common taxonomy and context in order to make the information relevant to the situation and the needs of the audience. This capability is critical, for example, in supporting coordinated efforts across multiple organizations in response to incidents.
- ☒ **Physical security of people or infrastructure** via monitored access and staff ID systems.

Much of the effort for homeland security, not the least of which is the development of standards and best practices, still lies ahead. The first responder community encompasses fire, law enforcement, public health, FEMA, and volunteer organizations. The work of defining a common vocabulary among these communities, identifying what information should be made available, and setting standards for how this data will be integrated and shared still remains to be done. Those companies that have an established government presence will be called upon to help set those standards, share best practices, and refine evolving homeland security systems.

City of New York Case Study: A GIS System That Evolved into a First Responder System

About 80% of all data collected by governments includes some type of location or spatial component, such as addresses, ownership records, maps, physical infrastructure details, zoning information, and more. Geographic information systems (GIS) offer an effective way to organize, present, and navigate this data.

PlanGraphics, a company that has built more than 5,000 GIS implementations for government and corporations, has worked with New York City (NYC) on its GIS needs since 1994. An initial effort to develop a citywide infrastructure warehouse has evolved into an ongoing project involving a dozen different government agencies.

The NYC GIS warehouse is a premier example of the role that location-based technologies can play in making public-sector data available to first responders. These geolinked technologies were used many times immediately after the terrorist attacks of September 11, 2001, and during the cleanup of the World Trade Center site.

One such application, developed with the NYC Mayor's office, is the *Emergency Management OnLine Locator System*. The original purpose of the system was to provide citizens with online access to information on emergency shelters and evacuation routes. Just one month after the system was launched, it was used extensively for onsite decision support near Ground Zero. Previously mapped information about the area around Ground Zero proved crucial to the fire department's search, rescue, and recovery operations. For example, the maps showed the location of underground storage tanks and access tunnels and also helped pinpoint utility hubs so that replacement systems could be installed.

Oracle Enterprise Database Spatial Utility is at the core of the current, full New York City GIS warehouse. Oracle and third-party tools are used for query and data extraction. Reports can be generated directly, or datasets can be "published" by specific rules and then overlaid on GIS applications. Data display can be handled by ESRI, Smallworld, MapInfo, Intergraph, and other mapping, presentation, and graphical user interface applications.

Just as important as the technical solutions are the powerful lessons learned from the project. State, local, and federal governments must have procedures in place for all types of disasters *and* be able to quickly locate and display the information they need to confront an emergency. Without procedures and intelligence, actionable solutions can be limited and the risks of serious mistakes increase. New York City decided that a GIS display of data was the best approach to the 9/11 emergency, and that decision helped speed recovery efforts.

Using the lessons learned in NYC, PlanGraphics now offers a quickly deployable solution architecture for location-based intelligence known as Spatial Templates for Emergency Preparedness (STEPs). With a focus on homeland security and critical infrastructure protection, STEPps can be easily adapted for broader government use.

Justice and Intelligence-Gathering Case Study: Real-Time Information Access, Profile, and Identity Matching

The Department of Justice and federal intelligence agencies often have a need to drill through multiple data sources to look for behavior patterns or personal associations that hint at terrorist activity. Because most of these installations are classified, this case study focuses on some specific applications used to help with this effort.

Las Vegas-based SRD offers a series of products that looks deep into multiple data sources in search of specific names, patterns, shared resources, or other information that can link people and places or indicate that one person is using multiple identities. SRD got its start tracing healthcare fraud cases, then developed algorithms used by Las Vegas casinos to trace suspicious activity and check visitor names against lists of wanted individuals or known felons.

SRD now offers several products that run in the Oracle environment. These products, which have been purchased and in some cases customized by government intelligence agencies, include a Non-Obvious Relationship Awareness (NORA) package that seeks obscure relationships between customers, employees, vendors, and other internal and external data sources. NORA analyzes patterns to determine potential threats or potential intelligence value. In some intelligence applications, data sources can include rental and real estate records, credit card and bank statements, telephone records, travel information, and other sources that could indicate when individuals are trying to hide or disguise their identities. NORA allows government agencies to find hidden relationships and suspicious activity that otherwise may not be noticed.

ANNA is another SRD product that looks for anonymous relationships between entities. It can know very little about people and still seek suspicious patterns. ANNA also has a unique feature that addresses many privacy concerns because it can share data and search for matches anonymously while information is still encoded. This capability makes it much easier for businesses to share records with the

government and with each other without violating privacy rules. If a match is found, say between an airline passenger and a terrorism suspect, the government could then seek a court order to view the full airline records for just that passenger.

Security Case Study: Crisis Management Center

Crisis management tools and techniques are crucial to first responders. Ship Analytics, a division of L-3 Communications Corporation, has developed L-3 CRISIS, a suite of software tools and professional services that can be employed in an emergency.

The CRISIS solution evolved out of a system designed to coordinate a response to oil spills. A unique piece is a built-in "fate and trajectory" hazard model that helps predict the outcome of certain events, such as oil spills or biological or chemical hazards. The system provides a suite of tools for an incident management team, including communication coordination, a GIS view of relevant data and an interface into relational databases that facilitate real-time data exchange between multiple components. Additional capabilities include response resource allocation, tracking, and cost accounting; message management; automated checklists; incident action logs; environmental and economic damage assessment models; countermeasure deployment assessment models; briefing tools; and image and reference libraries.

Several state and local governments are already implementing L-3 CRISIS. South Carolina is conducting a pilot study of the crisis management system. The state of Kentucky has made the L-3 CRISIS system available statewide, and Nassau County in New York is using the system on a limited basis with a hospital consortium.

Implementation Model: New Jersey State Police Office of Emergency Management Improves Responsiveness with an Oracle Database

On September 11, 2001, the New Jersey State Police Emergency Response Urban Search & Rescue Team, New Jersey Task Force 1, responded to the scene at Ground Zero within three hours. Other New Jersey State Police assets also provided essential support to New York City in the wake of this tragedy. The events of the day caused the New Jersey Office of Emergency Management (OEM) to take stock of its resources and develop a plan for more quickly mobilizing resources.

The Situation: Taking Stock of Emergency Resources

Separate emergency management communities exist within states, counties, municipalities, volunteer groups, and private sector organizations. Although relatively small in area, the state of New Jersey has 21 counties and 566 municipalities. Most of the municipalities have a police department and at least one fire department as well as ambulance services, mobile intensive care units, parks departments, public health organizations, private healthcare providers, and public works departments. Each of these organizations has resources and people with response capabilities that may be required in an emergency such as a natural disaster or a terrorist attack.

The problem was that each community had its own means of tracking and keeping inventory of its various resources. To quickly and effectively respond to an emergency situation, the state needs to know what resources and capabilities are available and where they are located. According to retired New Jersey State Police Captain Howard Butt, now working as a civilian emergency response specialist with the New Jersey State Police, "In a crisis, time is always of the essence. The faster the response to an emergency, the better, but you have to know what resources you have before you can respond." The New Jersey Office of Emergency Management responded to this problem by developing a Master Resources Database.

The Solution: A Statewide Master Resources Database

Beginning in spring 2003, the New Jersey OEM began to create a common statewide database of all of the resources across the counties, municipalities, and departments. The database will be able to track equipment and trained personnel and identify the location and status of each item through a common interface. It is similar to a supply chain management system that tracks and manages the resources available for emergency response.

The state began the database project with internal staff but quickly realized that it did not have the internal technology skills or time to manage such a massive undertaking. Some of the technology requirements and challenges that the New Jersey OEM faced include:

- ☒ Ensuring security of the database information
- ☒ Simplifying data entry procedures
- ☒ Developing a simple process for updating database records
- ☒ Developing the database using common terminology (resource typing)
- ☒ Allowing remote access and controlled information views

Through a connection with the New Jersey Business Force component of the Business Executives for National Security (BENS), an organization chartered with mobilizing the private sector to partner with the public sector, the New Jersey OEM connected with Oracle to help the state develop its Master Resources Database.

The New Jersey OEM partnered with Oracle to develop the database on the Oracle 9i platform. Oracle began by developing the database in Java, but within four months, the New Jersey OEM's requirements became more evident and Oracle decided to use HTML DB to program the database, which allowed for increased flexibility and a more streamlined approach to data entry. The Master Resources Database is a Web-based solution that allows appropriate access to state, county, municipal, healthcare, and volunteer organizations and private sector companies. According to Butt, "Oracle has provided an invaluable public service through the technology skills and support they have provided for this project."

The Master Resources Database is about 75% completed. For development purposes, Oracle has hosted the database in its own datacenter. However, as the database nears completion, Oracle will transfer the database system to a State Police data facility for security reasons. Critical and sensitive emergency response asset information must be maintained and secured by a government entity.

The response to the database has been extremely positive. It will provide a much-needed resource and assist all local and state government organizations to become equally prepared to respond to an emergency.

Benefits of the New Jersey Master Resources Database

Because of the database and the assistance provided by Oracle, the state of New Jersey will have the capability to access and act on valuable information that will help all of the state organizations respond in an emergency — natural or man-made. Whenever and wherever a disaster strikes, anyone with access to the New Jersey Master Resources Database can retrieve information on capabilities and identify all of the resources available to respond. The state not only can keep track of its response capabilities, it also can plan for a response to foreseeable incidents such as hurricanes. According to Butt, "New Jersey will have a safer and more prepared state, county and municipality system." Some of the specific benefits and features of the Master Resources Database include:

- ☒ **Reduction of response time.** Prior to the creation of the Master Resources Database, much of the communication was accomplished via word of mouth. With a one-stop database accessible by groups across the state, New Jersey will be able to reduce its response time by eliminating the time to search for which teams and equipment are available to respond. The database shows what is available, where it is located, and the time to respond based on the location of the incident and resources.
- ☒ **Comprehensive inventory.** The Master Resources Database will include a comprehensive inventory of all of the equipment and people available to respond to a disaster. The database will include not only an inventory of resource capabilities but also up-to-date information on training records, special skills, and contact information for personnel. This feature will be particularly useful for locating first responders if a particular skill is required in an emergency.
- ☒ **Greater cooperation.** The database will use common terminology and a standard language and format so that all agencies know what is available statewide. Through a shared resource agreement, local governments can avoid duplicating expensive items such as helicopters that are not used daily.
- ☒ **Flexibility.** The database will have the capability and flexibility to adapt to new assets and import data from all government organizations without reprogramming.

- ☒ **Validation of data.** A database is only as valuable as the data contained within it. The Master Resources Database will be dynamic — that is, every resource within the database will have a validation code based on how critical the resource is. Each department/organization will have a validation coordinator who must update the status of the resource based on its value in an emergency situation. The database automatically sends reminders to the coordinator when the resource must be validated. For example, a helicopter, which is a high maintenance and high-demand resource, would have to be validated weekly. On the other hand, a dump truck may require validation only every six months.

IDC Opinion

The battle against terrorism includes two different information wars. The first is the war waged by intelligence-gathering organizations such as the Defense Department, the CIA, the NSA, and the FBI — with help from local police and fire departments and government data collectors. The second is the war fought by first responders to have access to the information they need to do their jobs.

Secure access to accurate information is of paramount importance for both of these information wars. Only vendors that provide highly reliable, fault-tolerant systems and secure access to applications and data should be considered for this mission-critical effort.

The effort to build a highly reliable homeland security trusted information grid should start with the establishment of a solid foundation that can be accessed at the local level. Such systems need to be affordable, secure, reliable, and scalable. They should provide first responders with a single log-in system that provides access to law enforcement and fire department contact points, census, topographic and emergency management maps, transportation and public infrastructure data and grids, and views of any data that is relevant to their mission.

Oracle is in a unique position to provide technology solutions for homeland security efforts. It already has a large installed product base in federal, state, and local offices. It also has an existing set of applications for data sharing and a set of tools that is useful for developing highly secure mission-critical applications — applications that make it difficult for hackers to penetrate government systems. (Although no system is totally hacker-proof, secure Oracle databases and applications can serve as a trusted environment in which to develop and deploy mission-critical applications.)

The challenges for Oracle in this market space are price and complexity. System installation and application development are intricate when compared with cheaper and simpler tool sets. However, those particulars are also what gives Oracle the flexibility needed to tackle extremely large and complex installations. First responder systems and large applications capable of merging multiple data sources are not turnkey products. They have to be heavily customized, and Oracle's current product suite, including iHub, helps meet this challenge.

Conclusion

The big challenge for homeland security efforts in the months ahead will be to establish highly functional systems that allow government agencies to call upon all available resources; for example, first responders calling on emergency systems and personnel or intelligence agents calling on all of the public and private data that may reveal hidden clues about terrorist operatives.

The common need for all of these projects is the ability to build systems that can handle the import and display of data from multiple sources. The goal is to put the right information in the right hands as quickly as possible so that the homeland continues to stay secure. Because these homeland security solutions are a new breed of applications and they need to be mission critical, it is likely that governments will spend what they need to get them working and to keep them secure.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2004 IDC. Reproduction without written permission is completely forbidden.