

Operational Collaboration:

**The Role of Collaboration Technologies in Supporting the
Homeland Security Mission of Justice and Public Safety Agencies**

CRA Reports

*This report was prepared by
CRA Reports, an independent
reporting agency based in
Washington, DC.*

**Copyright © 2005
All rights reserved**

Operational Collaboration:

The Role of Collaboration Technologies in Supporting the
Homeland Security Mission of Justice and Public Safety Agencies

By

Lane F. Cooper

CRA Reports

This White Paper explores the state of Operational Collaboration among agencies at the federal state and local levels tasked with responding to Homeland Security threats. This report demonstrates how collaboration technology can contribute to the optimization of the Homeland Security operations by creating joint command, control, communications and intelligence platforms.

Much progress has been made since the tragic events of 9/11 to establish multi-jurisdictional collaboration networks that support federal, state and local agencies tasked with Homeland Security missions. Interviews with current and former government officials, technology partners in industry, and independent analysts tracking collaboration in Homeland Security, reveal that first responder organizations are adopting new technologies to better communicate and share information to thwart attacks or rapidly respond to specific incidents.

However, the level of operational collaboration is somewhat spotty. For instance:

- Urban and suburban regions with high population densities are much further along than rural low-density environments.
- Law enforcement agencies appear to be taking a more aggressive lead in forming regional centers for collaboration with federal, state and local entities than healthcare institutions and emergency response organizations.

Also, in states that regularly get natural disasters [like Florida and California], operational collaboration with sister agencies in different jurisdictions [sometimes different states] is quite good. But in areas where there is not much cause to work with other agencies or jurisdictions, collaboration infrastructures are much more limited.

Since Homeland Security preparedness is only as strong as its weakest links, the inconsistent application of strategies that harness collaboration technologies to prepare for and respond to emerging threats creates vulnerabilities. Among the operational risk factors that authorities should address are:

- **Inter-Organizational Integration and Communication.** In many crisis situations, first responder agencies (police, fire departments, emergency medical teams, etc.) still do not exchange information with sister agencies across jurisdictional lines in an efficient or effective manner because each agency tends to have communications and information processing systems that are incompatible.
- **Routine Collaboration.** In non-crisis situations, many agencies at local, state and federal government levels still have problems sharing critical information --

such as intelligence -- because of both technological and policy-based incompatibilities. This creates blind spots in the effort to prevent terrorist or criminal events from taking place. It also reduces the ability to develop effective plans to mitigate the effects of events should they take place.

- **Fiscal Pressure.** Many state and local agencies still do not have access to the financial resources necessary overhaul their systems and integrate them with sister agencies at the local, state and federal government levels.

...Homeland Security Community Responds with Opt-In Model

Another major barrier to comprehensive operational collaboration revolves around establishing who takes the lead in developing a national strategy.

While many participants in this community of interest have looked to the federal Department of Homeland Security (DHS) to create mandates and enforce standards, other jurisdictions have noted that progress made at the local and state levels of government that can serve as useful models for collaboration.

In an effort to strike a balance between providing some centralized leadership while simultaneously supporting local autonomy, members of the Homeland Security community -- which includes institutions representing federal, state and local agencies -- have launched an array of initiatives.

Most recently, a National Information Exchange Model (NIEM) program has been established by the federal Homeland Security and Justice Departments to test standards for data sharing and interoperability among federal, state and local agencies.

Other efforts to encourage voluntary participation in a national system of collaboration include the expansion over the past year of the DHS Homeland Security Information Network (HSIN) initiative. It has expanded its computer-based counterterrorism communications network to all 50 states, five territories, Washington, D.C., and 50 other major urban areas to strengthen its two-way flow of threat information.

The system is designed to deliver real-time interactive connectivity among state and local partners and with the DHS Homeland Security Operations Center (HSOC) through the Joint Regional Information Exchange System (JRIES). In this system, each state and major urban area's Homeland Security Advisor and other points of contact receive software licenses, technology, and training to participate in the information sharing and situational awareness that JRIES brings to state and local homeland security personnel across the United States. Examples of participants in the network include state National Guard offices, Emergency Operations Centers, and first responder and Public Safety departments at municipal and county government levels.

The expanded HSIN is also plugging into other communications networks used by law enforcement and other communities. For instance it is connecting to the Regional Information Sharing System (RISS) network, which is composed of six regional centers that share intelligence and coordinate efforts against criminals that operate across jurisdictional lines.

...Harnessing the Homeland Security Infrastructure

In short, the expanded HSIN is a network to which agencies with homeland security missions can apply to connect. It is a shared resource that not only makes information available to appropriate organizations, but also gathers data into a meta repository where information can be parsed and analyzed to understand the constantly changing nature of threats.

Simply plugging into HSIN -- or other local security/law enforcement consortiums, such as the Tampa Urban-Area Conflict Analytic Network (TUCAN) or ALIAS the Alaska law enforcement information exchange -- is not enough, however. State and local agencies must determine how that information is used by agency employees and shared with other agencies in various jurisdictions.

Agency leaders need to consider how the information can be most effectively distributed to police officers in the street and/or emergency responders at a disaster site.

The technology agencies use must not only integrate and consolidate disparate systems but provide analytics as well. It should show trends and relationships. For instance, if a police officer has very sketchy information about a suspect or a situation, he or she should be able to enter information into a networked PDA and receive some analytical support.

"We had situation where a sheriff's department was transporting prisoners for trial. One prisoner got away, but police on the street near the courthouse were able to perform a query on the suspect using their Blackberry devices. They found out that someone he had committed a previous crime with lived in the area. They recaptured the prisoner in 45 minutes." -- Senior Technology Official in Local Law Enforcement Agency

...Technological Requirements for Operational Collaboration

In order to access national resources so that agencies can apply them effectively in specific regions, the technologies that underpin Operational Collaboration networks must meet four critical requirements:

- **Standards based.** A consensus has been achieved among senior officials at federal, state and local agencies that there is little room for proprietary technologies that do not integrate or interoperate with other enterprise network elements. Compliance with key industry standards is an absolute requirement for critical elements in collaboration networks. This ensures that data can be shared among participants in a defined community of interest. It also makes it possible for those resources to be available to other collaborative environments.
- **Web Services Based.** Broad participation in inter-jurisdictional systems means that first responders are likely to access and interact with the system from a wide array of technological environments. This heterogeneous environment can best be managed by creating a Web Services platform to which different participants in the community of interest can post and download operational information.

- **Highly Secure.** The very nature of the work performed by Justice and Public Safety agencies is sensitive. Data gathered, processed and analyzed in these agencies are often used to prosecute criminals, thwart terrorist attacks and/or track wards of the state. And since first responders tend to be in the field, strong authentication technology (including biometric access control measures, such as fingerprint scans) at the device level is needed. Device- and network-level security is a paramount concern.
- **High Availability.** The environments in which the collaborative networks are going to be used tend to be harsh. Whether it is a hazmat event or a hostage situation, it is imperative that the collaborative networks be available continuously to the first responders on the scene.
- **Flexible.** As new threats manifest themselves or new technologies evolve to enhance the collaborative process, the underlying technology must be able to adapt to support a constantly changing environment.

About the Sponsor:

Microsoft Corp.

This series of reports is sponsored by Microsoft's Public Sector Group. Microsoft is responding to the challenges outlined in this report by working with respected independent software vendors, systems integrators, and management consulting firms that have extensive experience addressing justice and public safety issues on Microsoft technology platforms.

Specifically, the Justice and Public Safety Microsoft® .NET framework uses standards-based technology to connect a variety of applications on systems from different technology providers, using different operating systems.

Microsoft supports this integration vision by providing solutions that match customer requirements at every level of computing. This includes the Tablet PC and device-level operating systems (Windows® CE®, Windows XP Embedded, for example), through the desktop (Microsoft Office, Visio®, etc.), and continuing into the enterprise (Windows Server 2003, BizTalk® Server, etc.).

The Microsoft .NET programming model introduces XML-based Web Services, which developers can customize for use in any Web environment. The .NET building block services provide extensible "megaservices," such as user identity, personalization, calendar, messaging and universal XML-based search capabilities. This programming model allows justice and public safety agencies to seamlessly provide new levels of information access for users.

The community of business partners that has teamed with Microsoft to address integrated justice initiatives around the world represents the best technology practitioners in the industry. Microsoft not only has relationships with partners that have international reputations, but also with regional partners that have demonstrated their ability to provide highly responsive solutions to local agencies. In short, Microsoft tools and infrastructure technology are widely available to support implementations that enhance response, mitigate risk and protect citizens in a fiscally responsible manner.

For more information, please contact a Microsoft representative to explore strategies that will prepare your agency to effectively meet these new challenges, or visit: <http://www.microsoft.com/resources/government/>