

# **Collaborative Analysis and Response Strategies:**

**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**

**Collaborative Analysis and Response Strategies:**  
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 how effectively agencies at the federal, state and local levels are analyzing and responding to the vast amount of threat factors faced by the nation. This report demonstrates how collaboration technology can optimize the analysis of data generated by multiple agencies, correlate threat factors, and provide an analytical basis for responding effectively.*

There are times when the difference between a peaceful afternoon in a metropolitan area and overwhelming, heart-rending catastrophe is as simple as connecting dots. In the wake of terrorist events, it is relatively easy to work backwards from ground zero to trace the sequence of events that culminate in tragedy. It is much more challenging to put in place the mechanisms that identify suspicious activities ahead of time.

Unfortunately, the threats to Homeland Security are neither obvious, nor easy to compile. There are no gathering clouds that can be easily identified. There are no clear trajectories that can be tracked and used to project new threats with specificity.

Indeed, the specific elements of activity that combine to violently manifest themselves in the form of an attack are hidden on purpose by those who would do the nation harm.

Nevertheless, early threat detection is the key to identifying and preventing attacks on U.S. citizens, infrastructures and institutions. And, today, collaboration is the key to early threat detection. This is because no single organization or level of government (federal, state or local) is in a position to capture all of the information that may provide clues to imminent attacks.

The good news is that a collaborative approach to information/intelligence gathering, analysis and response significantly increases the footprint of coverage by maximizing the eyes and ears that are available to identify suspicious activity. The bad news is that it introduces a level of almost paralyzing complexity to the intelligence analysis and response processes. It also exposes conflicts in policy and organizational culture clashes among different agencies in the various levels of government. These are conflicts which can derail efforts to comprehensively gather, analyze and respond to useful intelligence.

As in other aspects of Homeland Security operations, enthusiastic and voluntary cooperation among federal, state and local agencies is a pre-requisite for success. This is because the constitutional separations of powers empower agencies with different lines authority and responsibilities to and from discrete constituencies.

Local agencies are directly responsible to the local electorate. State government officials must account for their activities to state legislatures and voters. And federal authorities and bureaucracies are ultimately managed by an executive branch that is accountable to the nation as a whole.

Unlike other countries that deal with the threat of terrorism, there is no centralized national police or security force around which a hierarchical command and control structure can be wrapped to manage and channel the flow of intelligence.

This decentralized governance structure contributes to the vast system of checks and balances that contribute to the vitality of our democracy. But it also contributes to a tremendous heterogeneity that must be managed in a cooperative manner if the Homeland Security mission is to be accomplished.

### **...Addressing the Problem of Heterogeneity**

Agencies across the country have adopted and implemented a wide array of technologies that create, process and store data. As a result:

- Federal, state and local agencies have deployed technologies at different rates. This means that there are different generations of the same technological product lines in the environment.
- Agencies have embraced different technological philosophies. This means that a wide range of solutions from vendors with proprietary offerings may be in place. These technologies may not interoperate with standards-based systems or the unique characteristics of technologies developed by competing technology vendors.
- Different technical and operational imperatives have led to the development of various technical and operational terms of reference. In other words, as information in repositories are created, processed and stored in different technical and operational environments, the absence of common terminology contributes to confusion when data from multiple sources are pooled for analysis.

These and other technical issues create barriers to effectively aggregating, analyzing and responding to trends that can lead to terrorist attacks. But technical issues are not the only barriers to effective analysis and response operations. Different agencies have different missions which can lead to clashes of organizational culture. For example:

- Within the federal government, the law enforcement imperative (to gather evidence as well as intelligence for use in post-event prosecutions) continues to conflict with security and intelligence agency imperatives to protect methods and sources.
- State and local agencies may not have gone through the security clearance processes that govern “who, what and how” classified information from federal sources are accessed and used.
- Conflicting rules, regulations and policies that govern how information is accessed and use by different agencies in different states, counties and municipalities can inhibit the ability to share information.

### **...The Role of Collaborative Technologies**

Effective deployment of collaboration technologies to support information analysis and response operations in a multi-jurisdictional environment can address both the technical and organizational challenges. For instance, many of the technical interoperability hurdles are being addressed by broad adoption of standards-based web services architectures.

Web services are self describing applications that can discover and engage other web applications to complete complex tasks over the Internet. Legacy systems -- and other non-standard applications -- can "map" their fields and records to the web services applications, so that other computer systems can access resources. In other words, the web services platform becomes a single point of integration.

Thus, by strategically implementing web services technology, agencies can share information resources without having to completely overhaul legacy information systems. The development of the web-based Global Justice XML standard further facilitates information sharing by creating a common language for operational applications in the Justice and Public Safety arena.

Armed with these two technological developments alone (web services applications and GJ-XML) federal, state and local agencies not only have an opportunity to open up windows into previously "stove-piped" enterprise resources, but also can develop applications that allow knowledge workers to mine and analyze information in multiple systems simultaneously.

This provides the collaborative framework for analyzing intelligence and crime data, allowing agencies to more effectively prevent criminal or terrorist activities from taking place as well as support the forensic analysis process in the wake of an event. A good example of an application that harnesses these collaborative tools is an offering called CrimePoint2005, from Walnut Creek, Calif.-based Forensic Logic.

The web-based GJ-XML based software application helps law enforcement officers solve crimes and better allocate resources to reduce crime in areas of high crime incidence by combining three factors needed to solve a crime:

- Sophisticated database operations,
- Geographic visualization, and
- Matching of crime event data to patterns associated with suspect criminal behavior.

Using .NET web services technology from Microsoft, the CrimePoint2005 data sharing information management and analysis system can interact with servers from multiple agencies through web browsers. The application can coordinate the activities of a number of physical and logic servers and services. These servers and services:

- Retrieve real-time data from agency databases;
- Run analytical procedures on indexed data;
- Send and retrieve geographic information from map server; and
- Return results to analysts in an HTML format.

### **...Technological Requirements for Joint Analysis and Response**

To access national resources so that agencies can apply them effectively in specific regions, the collaboration technologies that underpin joint analysis and response operations must meet the following 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 analysts 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 web services platforms to which different participants in the community of interest can post and download operational information.
- **Highly Secure and Redundant.** There can be no collaboration without trust. There can be no trust if there are concerns about the security and integrity of information shared in collaborative analysis systems. The systems must be continuously available -- even in the midst of critical events. The collaborative environment must be seen as a reliable resource and reference to the operational collaboration systems that are responding to events in the field.
- **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 report 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/>