

# Homeland Security

## How Government Can Begin to Bridge the Information Gap

**I**nteroperability among government information systems is critical to winning the war on terrorism. The demands of homeland security dictate that federal, state and local government agencies remove the barriers that block exchange of vital data and services — and they must do so quickly and cost effectively.

“The current situation is that government systems can’t communicate,” said Frank Giebutowski, General Manager for Microsoft’s state & local government business. “There is a new vision for integrated homeland security; the question is, how do you bridge the political and technical realities to make it work?”

Although governments themselves must break down political and cultural barriers to interoperability, Microsoft and its partners offer a practical strategy for surmounting the technical hurdles. Working in concert with other software companies and standards organizations, such as the World Wide Web Consortium (W3C), Microsoft developed an approach known as the Government Interoperability Framework.

Based on a Web services model, the Government Interoperability Framework combines Internet-based standards, such as XML and Simple Object Access Protocol (SOAP), with robust security, a centralized service registry and agreements among agencies on data schemas. The result is a seamless, secure fabric of services that promotes data sharing among agencies and provides government with a crucial resource for winning the war on terrorism.

### A TALL ORDER

Sharing information between agency IT systems and among public jurisdictions historically has presented a tough challenge for government. The situation persists for a number of reasons.

Different systems often represent the same object in different ways. Where one system stores a person’s first and last

### RAMSAFE INTEGRATES MULTIPLE AGENCIES TO ENSURE SAFETY AT UTAH WINTER OLYMPICS

Concepts contained in the Government Interoperability Framework were proved during the 2002 Salt Lake City Winter Olympic Games. The Utah Olympic Public Safety Command (UOPSC) used a secure XML-based software and services platform to integrate information from federal, state and local agencies so that planners and first-responders could be rapidly briefed and deployed.

UOPSC’s security resources spanned many government anti-terrorism and emergency-response agencies, including the FBI, Secret Service, Department of State, Department of Defense, Health and Human Services, FEMA, and a series of state and local authorities. “Our need to create one central system that all of these officials could use at all locations, including mobile laptop units, was essential,” said Craig Dearden, Utah’s former commissioner of public safety. “We needed everyone on the same page.”

Microsoft partner RAMSAFE Technologies (RST), LLC of Marietta, Ga., met this need by creating a new generation situation-management and anti-terrorism system. The new technology — also known as RAMSAFE — ran on Microsoft SQL Server 2000, Microsoft Internet Information Server 5.0 and Internet Explorer, using XML for secure data sharing.

RAMSAFE was developed under a partnership between U.S. government and private-sector companies with substantial input from emergency managers and responders. It dramatically improves, but does not replace, existing emergency command center and incident commander applications. In particular, RAMSAFE strengthens planning and training, improves operational response, enhances situational awareness, and provides the resources needed to make proactive decisions.


For example, the system can retrieve pictures of buildings or room combinations from various databases, put them on screen, and allows users to draw on them like a white board. Users navigate rapidly between satellite photos, maps, building footprints, floor plans, individual rooms, photos and documents. In other words, RAMSAFE delivers vital support to first responders in pressure-packed emergency situations.

“In an emergency, that briefing capability alone would allow planners to more quickly and thoroughly prepare response teams before sending them in,” said Dearden.

In less than 60 days, UOPSC had implemented an enterprise solution encompassing all 22 Olympic venues, the Salt Lake City Airport and other related sites spread over 3,000 square miles. At the same time, RST trained 225 federal, state and local security officials to use the system.

What made this homeland security platform particularly effective was the fact that frontline responders could access the system securely from anywhere using only a laptop computer and Web browser. In addition, the platform allowed UOPSC to centrally coordinate the activities of multiple security agencies — from local to federal— across geographically dispersed sites. Virtual touring and testing capabilities helped officials hone response plans, and interactive briefing tools quickly prepared first responders for action.

For more information on this solution, go to [www.ramsafe.com](http://www.ramsafe.com)



names in separate data fields, another may store both names in a single field. Similarly, systems may use different codes to represent the same information. One system may use U.S. to represent the United States, but another may represent the term United States with the numeral 1.

Agencies also must ensure the security of exchanged messages and data, a requirement that typically dictates the use of some form of encryption. And they confront connectivity issues such as deciding which network and communications protocol to use.

These and other technical concerns combine to make interoperability much easier said than done. Moreover, an interoperability solution must meet a series of real-world government requirements if it is to succeed.

For example, the solution must allow agencies to participate in whatever manner they choose, instead of forcing compliance. This “opt-in” design is vital to implementing a trustworthy privacy policy. Agencies also must join the system with minimal impact to existing information resources, and the system must make it relatively easy to begin securely sharing data.

### **AN ELEGANT SOLUTION**

The Government Interoperability Framework uses the Web services concept and open Internet standards, such as XML and SOAP, to meet the interoperability demands of public jurisdictions. The Framework builds a solid IT infrastructure, institutes reliable security processes, promotes collaboration and data sharing, and seamlessly encompasses the huge array specialized government solutions offered by hundreds of Microsoft industry partners.

The Framework’s XML-based Web services architecture allows programs to communicate in a standards-based way — even if they are written in different programming languages and are operating on different computing platforms. The XML standard focuses on content and business context — instead of how the content is displayed or printed — enabling systems to exchange and interpret documents without human intervention. In addition, recently developed XML schemas reconcile the disparate tag structures, content and data types that are commonly encountered when agencies attempt to link together multiple information systems.

The Framework also includes security services designed to ensure that only authorized users gain access to sensitive data. These security services use a modular design and isolate agency applications from underlying user-identity technologies. Therefore, agencies can easily adopt new identification technologies without altering their applications.

Agencies participating in the Framework would control access to their data by granting access to groups of individual users. Additionally, agencies can choose the specific data they want to share or not share rather than the “all or none” approach most systems use today. This allows them to maintain full control over their data — even if shared with other outside agencies.

Finally, the Framework includes Request Manager servers that manage the flow of information among participating agencies and Document Interchange capabilities that give users additional flexibility for publishing information and notifying information recipients. Agencies also may add data-mining capabilities, analytical applications and other business intelligence tools designed to create knowledge from raw information.

### **AVAILABLE AND PRACTICAL**

The industry standards and products required to implement the Government Interoperability Framework exist today. Microsoft and its network of industry partners already are delivering solutions based on this concept.

Besides being available immediately, the Interoperability Framework is practical. Web services envisioned for the Framework can be added as a front end to existing applications, allowing agencies to implement a new level of data sharing without rewriting or replacing legacy systems. Furthermore, government organizations continue to own their data and control access to it. And, the system could use a variety of communications networks, including the Internet or a secure government intranet.

Clearly, information sharing and application integration are vital weapons for governments and first responders intent on winning the war against terrorism. With the Government Interoperability Framework, Microsoft offers a timely, practical and affordable strategy for arming agencies to protect the nation’s homeland.

**To receive more information about  
Homeland Security solutions or speak  
with a Microsoft representative,  
please call 202-274-7577.**

**Microsoft®**