



Homeland Security IntelWatch

January 2004
Vol. 2, No. 1



[National Homeland Security Knowledgebase](#)



Chairman:
Edward J. Krause, III,
CEO, E.J. Krause

Publisher and Editor-in-Chief:
[Michael Rosenberg](#),
Vice President,
Security, E.J. Krause

Editor, International Operations:
[Peter Buxbaum](#)

Deputy Editor:
[Steve Ellis](#)

Operations Manager:
[Lindsey Field](#),
E.J. Krause

International Operations/Business Development:
[George Debakey](#),
E.J. Krause

Sponsored By



Exhibit at the
U.S. Maritime Security Expo 2004

Interoperability

The ability for thousands of federal, state, and local law enforcement and emergency response organizations to interact with each other will be critical to an effective response to another 9-11. Promoting the interoperability of their communications and incident management systems has therefore taken center stage, not only in Washington, but in cities, counties, and states around the nation.

As the following articles suggest, efforts to enhance interoperability to date have been admirable. But true interoperability is still in an embryonic stage.

The rapid promulgation and acceptance of interoperability standards would go along way towards reducing the risk of private or public sector investment in any particular communication or emergency management technology.

An Emerging Standard for Emergency Interoperability?

A data standard that could provide interoperability to emergency communications systems is scheduled to be finalized before the end of the year. The Common Alerting Protocol (CAP), developed by the Emergency Interoperability Consortium (EIC), uses a version of the XML data language to allow different emergency communications platforms to simultaneously exchange public warnings.

"Currently, the emergency notification infrastructure in the United States is built on disparate systems," said Matt Walton chairman of the EIC and vice chairman of E Team, Inc., a Los Angeles-based company that makes a Web-based incident management application.

XML is a format increasingly used to transmit data over the Internet and other networks. CAP was formulated in conjunction with OASIS (the Organization for the Advancement of Structured Information Systems), an influential international XML-based standards body.

CAP provides a data format that allows a consistent warning message to be disseminated simultaneously over many different systems. It can be also used to detect forthcoming hazards or hostilities by detecting emerging patterns.

Veterans of the interoperability wars

EIC was formed "a little over a year go," said Walton, "when ten companies came together based



Matt Walton

Is there profit in public-private information sharing?

The answer is "yes," according to Charles Jennings, founder and chairman of RAINS, the Regional Alliances for Infrastructure and Network Security and chairman and CEO of Swan Island Networks, a Portland, Ore.-based provider of secure Internet communications.

Contact Information:

Tel 301-493-5500
Fax 301-493-5705

[Send us your comments.](#)

[To Advertise click here.](#)



on the understanding that interoperability was a real problem that had to be addressed. On 9-11, it became crystal clear that lives had been lost at the World Trade Center because of the inability of institutional responders to effectively share information with each other."

The consortium now has more than 70 members, including the Department of Homeland Security, the National Emergency Management Association, Boeing Corp., IBM, Unisys, Microsoft, and Oracle.

Walton and E Team are veterans of the interoperability wars. E Team had a contract to implement its incident management system at New York City's Emergency Operations Center (EOC), the deployment date to be September 17, 2001. When the World Trade Center was attacked on September 11, destroying the EOC, E Team accelerated its implementation, and got its system up and running at the new op center on a Hudson River pier within 72 hours. E Team's system connected more than 150 federal, state, and local agencies, nonprofit disaster relief organizations, as well as significant infrastructure providers such as Amtrak, Verizon, and Time Warner cable.

"We have a strong preference to deploy the system and interface it with various other systems in advance of a disaster," Walton commented.

E Team started in 1989 as an R&D contractor to the Defense Department. "Interoperability was recognized as critical by the Pentagon beginning in the 1970s," Walton said. "It truly became incorporated as a vital mission in 1980s and was realized in the 1990s. We participated in all of those transitions."

The civilian sector, in government agencies like FEMA, began to grapple with the issue of interoperability even before September 11, according to Walton. But, he said, 9-11 "brought the issue into stark relief."

CAP proof of concept

The EIC conducted a proof of concept for CAP at the end of September during which responder agencies in two cities, states, counties, and FEMA regions reacted to the simulated release of Sarin gas in St. Louis. "A single message was originated in CAP. That message was passed electronically to two different alarm systems, blasted out to tens of thousands of people via email, and automatically posted to several public websites," Walton said. "It also went out over incident management systems like ours, which immediately sent out notifications to predefined people from chiefs of police chief to departments of health."

In October, the first set of standards for CAP was published. Following a period of testing and public comment, the standards are scheduled to be

The first installations of an enterprise version of RAINS-net, an information-sharing system developed by Swan Islands and three other Portland-area hi-tech companies, are coming soon, he said.



Charles Jennings

RAINS was organized as an Oregon public-private partnership after September 11, 2001, as an effort to accelerate the adoption of information-sharing technologies that would ensure effective responses to emergencies. The organization received \$60,000 in state seed money.

RAINS-net, which was kicked off last summer, ties together the Portland 911 call center with the information systems of 60 entities, including government agencies, first responders, school administrations, hospitals, and private companies. The system grabs data from 911 calls and disseminates that information over the Internet, depending on the nature, severity, and geography of the incident, to appropriate participating entities.

RAINS has now packaged RAINS-net as an enterprise system for large corporations that seek to distribute incident information to employees and associates. An enterprise version was tested by the Hilton Hotel in Portland, and Jennings expects other installations to begin – with revenues to start flowing – in the coming months.

The package will be marketed by RAINS, and the revenues will stream back to the organization to pay its expenses, as well as to participating technology companies. "We see extension into the enterprise as a key component of the program," Jennings said. "We are carving out a unique niche which involves building bridges between first responders and infrastructure owners."

Field test for chem-bio response system

The Department of Homeland Security field

finalized this month.

"We are supporting a series of tests and validation exercises that will be used to establish the standards," said Walton. "Then there will be follow-up by consortium members to get the word out there that this capability is real."

How valuable is it?

For Dan Miklovic, a Seattle-based vice president and research director at Gartner/G2, a technology analyst firm, the CAP effort, although worthwhile, represents but the tip of the iceberg when it comes to first responder interoperability. "Sharing alert information across state boundaries is important," he said. "CAP has real value and is an excellent use of XML."

The real challenge, according to Miklovic, is in sharing information prior to an alert being generated. CAP alerts are "post event," he said, "and there are a whole lot of other activities and messages that need to be dealt with. The challenge is driving it down to the level of cop-to-cop or cop-to-EMS communication."

For his part, Walton hopes that CAP will end the "paralysis in the emergency management community around making a commitment to a particular system."

"They don't want to embrace something they can't interface with," he said. "With the emergence of real standards, they can be assured that whatever they are committing to is not going to be dead ended. That is a huge step forward."

tested the Chemical Biological Response Aide (CoBRA), an emergency response system, in an exercise last month in and around Port Newark, N.J., that included 600 federal, state and local emergency workers from 70 different organizations. The exercise simulated responses to chemical and radiological leakages from containers unloaded at Port Newark.

"The exercise was the culmination of three years of planning that started pre-9/11," said Dr. Don Ponikvar, senior vice president at the Defense Group Inc., of Alexandria, Va., the developer of CoBRA.

CoBRA, which includes software and ruggedized laptops, automates the collection of data during an emergency and wirelessly makes it available to responders and others. "CoBRA offers a data interchange standard so that threat and incident information can be exchanged," said Ponikvar.

CoBRA also includes an electronic reference library for chemical, biological, radiological, and explosives threat data, a collection of government best practices and local unit protocols for responding to incidents involving weapons of mass destruction, a set of interactive checklists to guide actions on-scene, and an automatic time-tagged event log for all responder actions.

Organizations participating in the New Jersey exercise included local and county first responders, the New Jersey State Police, and federal agencies such as the FBI, the Bureau of Customs and Border Protection, the Coast Guard and FEMA.