

# CRISIS INFORMATION MANAGEMENT SOFTWARE (CIMS) INTEROPERABILITY

## *A STATUS REPORT*

INSTITUTE FOR SECURITY TECHNOLOGY STUDIES



© Copyright October 2004, Trustees of Dartmouth College. All rights reserved. This project was supported under Award No. 2000-DT-CX-K001 from the Office for Domestic Preparedness, U.S. Department of Homeland Security. Points of view in this document are those of the author(s) and do not necessarily represent the official position of the U.S. Department of Homeland Security.

Technical Analysis Group  
45 Lyme Road  
Hanover, NH 03755  
(603) 646-0700  
[www.ists.dartmouth.edu](http://www.ists.dartmouth.edu)

# CRISIS INFORMATION MANAGEMENT SOFTWARE (CIMS) INTEROPERABILITY

## *A STATUS REPORT*

INSTITUTE FOR SECURITY TECHNOLOGY STUDIES



© Copyright October 2004, Trustees of Dartmouth College. All rights reserved. This project was supported under Award No. 2000-DT-CX-K001 from the Office for Domestic Preparedness, U.S. Department of Homeland Security. Points of view in this document are those of the author(s) and do not necessarily represent the official position of the U.S. Department of Homeland Security.

Technical Analysis Group  
45 Lyme Road  
Hanover, NH 03755  
(603) 646-0700  
[www.ists.dartmouth.edu](http://www.ists.dartmouth.edu)

## TABLE OF CONTENTS

<b>Executive Summary .....</b>	<b>1</b>
<b>Introduction.....</b>	<b>5</b>
<b>Object of the Study .....</b>	<b>6</b>
<b>Key Definitions .....</b>	<b>6</b>
<b>Methodology .....</b>	<b>6</b>
1. Select an Advisory Panel .....	7
2. Literature Review.....	7
3. Vendor Survey .....	7
4. Practitioner Workshop .....	8
5. Data Analysis and Report Production.....	9
<b>Findings and Analysis.....</b>	<b>10</b>
CIMS Definitions and Terminology .....	10
CIMS Interoperability.....	14
Interoperability Challenges.....	20
Recommendations to Move Interoperability Forward.....	22
<b>Advisory Panel Members .....</b>	<b>27</b>
<b>Bibliography .....</b>	<b>28</b>

## EXECUTIVE SUMMARY

A lack of overall situational awareness is often cited as a key challenge for decision makers and responders alike. This report, *Crisis Information Management Software (CIMS) Interoperability: A Status Report*, examines the status of interoperability between the Crisis Information Management Systems (CIMS) that help manage the flow of critical event data in many emergency responder organizations.

It is unclear how broadly CIMS are adopted across the Nation. We found no statistics on CIMS adoption by organizations in the public or private sector, however, larger population areas seem to be more likely to have adopted CIMS. Additionally, we found that larger population areas are pursuing forms of regionalized information and resource sharing. Specialization of products to sectors was not generally found; for the most part vendors told us that their products are designed for all-hazard response. The Nation's unique system of federal government and local autonomy allow great flexibility in individual CIMS purchasing decisions. As a result, we discovered that a variety of products have been adopted by organizations to fit their particular needs.

The issue of interoperability between emergency management and disaster mitigation organizations is larger than just the CIMS component. Many systems provide a plethora of Command, Control, and Communications (C3) information that extend the use of CIMS. Such programs would include Geographic Information Systems (GIS), weather and plume modeling, aerial photography, street mapping, and real time closed-circuit television data. We acknowledge here that examining the breadth of issues surrounding interoperability between all levels of C3 software is well beyond the scope of this report. Overall we note that CIMS adoption and use involves the coordination of many disciplines and information must be mapped across communities and sectors. Less sophisticated partners need to be able deliver information to, and obtain information from, the more sophisticated users' CIMS.

Future CIMS definitions should be expanded to include specific functional areas and include other critical infrastructure sectors. At this time there is no broadly accepted vocabulary of technical terms for use with CIMS. Without such a terminology, members of the community, including practitioners, vendors, and academics, will continue to struggle at all levels of interoperability development. Practitioners we spoke with expressed the need for efforts to determine what information or "data elements" need to be exchanged across jurisdictions and disciplines.

Our research indicates that since 2001, a number of efforts have been undertaken that may assist the interoperability of CIMS. Government entities are involved with coordination efforts and have produced actual software tools. Strategic reports, methodologies, and standards are being produced by non-governmental organizations.

Communications interoperability requires the coordinated efforts of leadership at the local, state, and federal levels. While most users believe agencies within state governments have stepped forward, they are looking for more emphasis on Federal and interstate coordination. We estimate that from a practitioner's standpoint, the

government's assignment of responsibilities regarding interoperability has neither helped nor hindered efforts to increase CIMS interoperability to date. At this time, the government's efforts are ongoing and time is needed to determine the affect they may have on CIMS interoperability.

Our studies participants did note that government efforts may take longer to develop and may be less responsive to community needs than private sector developments. To address timeliness and responsiveness, both practitioners and vendors advocated the use of public/private partnerships to drive government sponsored or government sanctioned standards efforts. The consensus of our research subjects is that government efforts must be relevant to make a difference. By bringing parties involved together and developing a framework for CIMS interoperability, the government may facilitate rapid developments toward better situational awareness capabilities for emergency managers.

The survey we conducted during this study indicates that vendors are currently involved in standards organizations and various consortia dedicated to improving CIMS interoperability. Most vendors in our survey said they are ensuring products meet current and developing industry methodologies and standards; and plan to be compliant with a growing number of industry methodologies and standards in the next three years. Additionally, interviews with vendors indicated that some vendors are participating in CIMS interoperability demonstrations.

From a vendor perspective, CIMS are both relatively interoperable and intraoperable. All of the vendors in our survey told us that computers or servers within their CIMS program can share data with each other. Survey respondents indicated the most common method of data transfer used to share data within CIMS programs is the Internet Protocol (IP). The eXtensible Markup Language or XML is the most common language for the interchange of structured data found in our survey. The majority of the vendors in our survey used XML for both data import and export.

The practitioners involved in this study related that many emergency response organizations simply do not use CIMS. Possible reasons we identified from our structured interviews with emergency managers and practitioner workgroup are 1) cultural resistance to adopting Information Technologies (IT); 2) lack of IT resources; 3) information technologies may not be considered in planning processes or are not a priority equipment purchase.

Vendor responses in our survey indicated that all CIMS use databases to store data. This led us to ask the question "Is the interoperability of CIMS really a database integration issue?" The practitioners in our study commented that if CIMS interoperability was simply a data fusion issue it would have been solved already. For example, our practitioners described cases when interoperability was established between CIMS over secure lines and yet little data was shared. Why did these events occur?

The participants were asked to comment on these cases and noted that there are "cultural issues" that affect information sharing. When incidents occur information is often shared through informal backchannels such as phone calls and emailed documents. Our practitioners commented that in some circumstances individuals don't wish to lose control over their information. Owners of information want to control who sees data and to whom users can send their data. Our workshop participants noted a hesitance in

sending sensitive information to someone you do not personally know, regardless of the security of the transmission medium itself.

To address the issues we outline in this report recommend the following:

1. **Establish a national practitioner working group to develop a standard CIMS terminology and consensus-driven user-defined needs.** Based on the research we conducted, we conclude that a practitioner working group with the goals of developing a CIMS terminology and consensus-driven user-defined needs is a missing component of the framework needed to facilitate change nationally. Throughout our research, members of the vendor and standards community both expressed that greater clarification on the user's needs regarding interoperability is required. This is particularly required in light of new national imperatives such as the National Incident Management System. Without clear definitions of the roles of responders and clear delineations placed on the information flow, it is difficult to memorialize the management of incidents and events into software code.
2. **Coordinate standards efforts across critical infrastructure sectors.** The participants in our study told us that future definitions of CIMS need to be expanded to include other user groups across critical infrastructure sectors. We note here that many of the standards efforts that are underway are sector-specific, yet overlap into other critical infrastructure sectors. The consensus of our study participants is that it is in the best interest of the responder community as a whole to coordinate standards efforts to limit redundancy and to maximize the vendor's standards compliance efforts. The Department of Homeland Security has the mandate to undertake this effort.
3. **Develop incentives to encourage vendor compliance with standards as a key driver towards CIMS interoperability.** If the parties that develop and use CIMS can work with government to develop a common set of standards across critical infrastructure sectors then incentives can be developed to drive interoperability. For example, if data exchange structures were defined and sanctioned by the Federal government, grant monies could be tied to their implementation. Vendors and practitioners alike would benefit by having a common base to build upon when purchasing, implementing, and maintaining CIMS.
4. **Interoperability must be a priority in the CIMS purchasing process.** Throughout our research we have encountered CIMS users that placed interoperability low on their list of requirements. Once the systems became operational, data sharing needs quickly moved to the forefront of users' requirements. We encourage prospective CIMS purchasers and those upgrading their systems to place a greater relative priority on interoperability during their requirements analysis. We believe that without this change in thinking a general lack of interoperability will continue to cascade across CIMS implementations.
5. **Develop purchasing guidelines.** In order to help organizations integrate interoperability thinking into their purchase or upgrade processes we provide simple guidelines regarding CIMS interoperability to assist organizations when

building purchasing requirements. More detailed purchasing guide lines would be of great use to responder agencies.

6. **Promote CIMS interoperability goals in exercises and create a repository for lessons learned.** During our research we discovered that there were situations where the technical ability to share information securely existed, but information was not shared due to social and cultural factors. We believe one of the most effective ways to combat this dilemma is through exercises and simulations. Including CIMS-specific tests and goals in exercises will be a critical first step however other components are needed to ensure that the lessons learned are made available to the people who need them. We support our study participants' position that a national repository of after action reports and lessons learned should be created. Such a resource does not exist today. The creation of a one-stop-shop for CIMS-related materials would significantly increase the ability of both sophisticated and new user organizations alike to develop their understanding and use for CIMS.
7. **Initiate research into data security, including permissions and trust, in CIMS interoperability.** When the technical problems regarding interoperability are removed, other problems become apparent. One of these problems is the issue of data security, including permissions and trust. If an interoperable system of systems is developed, a process for authenticating users, setting user access rights, rights of users to access materials and add other users must all be considered. Practitioners and vendors alike are concerned about the security of their data. We recommend that research be conducted into the issue of permissions and trust before it becomes a limiting factor in interoperability.

## INTRODUCTION

Terrorist attacks over the last decade have grown in violence and sophistication, culminating in the devastating attacks of September 11. The threat of terrorist attacks against U.S. citizens and U.S. interests around the world has become the Nation's most pressing national security issue. Several expert commissions, and the first responder community alike, have addressed the threat of terrorist and made specific recommendations to enhance their efforts to prevent and respond to terrorist acts. These groups have called for broader use of technology to assist in emergency incident management.

The Institute for Security Technology Studies (ISTS) at Dartmouth College is dedicated to pursuing research that addresses critical national needs for security technology and policy in cyber and emergency response environments.<sup>1</sup> The interdisciplinary ISTS teams of academic scholars and professional scientists investigate critical security problems, both through the creative application of existing technology and ideas, as well as through the discovery of new knowledge and the development of new technology. The interdisciplinary nature of the teams allows them to tackle problems from a variety of perspectives including science, engineering, social science, and policy.

New technologies are providing advanced capabilities to many responder agencies. This is especially true in the area of situational awareness. The *9/11 Commission Report* identified a lack of overall awareness as a key challenge for decision makers and responders during the 2001 terror attacks on the United States.<sup>2</sup> Even with the multitude of sensors and communications devices possessed by our responder communities, an overall picture of events on the ground was hard to maintain. Many response organizations are deploying Crisis Information Management Systems (CIMS) to help manage the flow of critical event data.

CIMS are often defined as the software commonly found in emergency operation centers that support the management of crisis information and the corresponding response by public safety agencies.<sup>3</sup> When used to their full potential, CIMS can increase first responders' operational response and situational awareness and can help central command and control facilities communicate and coordinate the activities of multiple agencies preventing delays, confusion, and ineffective responses. In this report, we examine the current status and challenges that surround the ability of CIMS to share data.

---

<sup>1</sup> For more information on the Institute for Security technology Studies at Dartmouth College please see URL <<http://www.ists.dartmouth.edu>>.

<sup>2</sup> National Commission on Terrorist Attacks Upon the United States, available at URL <<http://www.9-11commission.gov>>.

<sup>3</sup> *Crisis Information Management Software (CIMS) Feature Comparison Report* available at URL <<http://www.ojp.usdoj.gov/nij/pubs-sum/197065.htm>>.

## OBJECT OF THE STUDY

In 2003, the Technical Analysis Group at ISTS met with the Department of Homeland Security's Office for Domestic Preparedness (ODP) to determine priority research areas.<sup>4</sup> ODP requested we conduct a study of CIMS and their ability to share data. A 2001 report, titled *Crisis Information Management Software (CIMS) Feature Comparison Report*, noted no significant efforts underway for standardization in the different software products.<sup>5</sup> Further, the report finds that the automated exchange of information between agencies using different products will continue to be problematic without intervening efforts to develop and promulgate standards.

This report addresses the following two questions:

1. *What is the current interoperability of CIMS?*
2. *What steps may be taken to improve interoperability between CIMS?*

## KEY DEFINITIONS

In order to ensure continuity in our research, we chose to adopt specific definitions for CIMS, Interoperability, and Intraoperability. This is especially useful since interoperability has different meanings for different sectors of the emergency management and response community. The definitions we use are as follows:

**Critical Incident Management Software (CIMS):** CIMS are programs specifically designed to support incident or event information management functions for federal, state, and/or local emergency management.

**Interoperability:** For purposes of our research interoperability is defined as the ability of disparate CIMS to exchange information and services directly and effectively between each other and their users.

**Intraoperability:** For purposes of our research intraoperability is defined as the ability of identical CIMS to share information.

## METHODOLOGY

The research for this study was conducted over nine months from February to October 2004. The five major steps in our research are as follows:

1. Select an Advisory Panel
2. Literature Review
3. Vendor Survey
4. Practitioner Workshop

---

<sup>4</sup> For more information on the Department of Homeland Security's Office for Domestic Preparedness please see URL <<http://www.ojp.usdoj.gov/odp/>>

<sup>5</sup> *CIMS Feature Comparison Report*, <<http://www.ojp.usdoj.gov/nij/pubs-sum/197065.htm>>.

## 5. Data Analysis and Report Production

The following passages provide an overview of our methodology.

### **1. Select an Advisory Panel**

Working with ODP, we conducted an extensive outreach effort to recruit an expert practitioner advisory panel. The primary purpose of the panel was to provide critical guidance throughout the duration of the project. The group of seven individuals we selected represents a broad segment of the emergency response community from the federal, state and local levels. The advisory panel assisted us in identifying key resources in government, academia, industry and the emergency response community to help us meet project objectives. A complete list of advisory panel members is included on page 27 of this report.

### **2. Literature Review**

A comprehensive review and analysis of previous research and related authoritative literature was the first step in this study. Before beginning the literature review, ISTS researchers took a number of foundational steps which included; consultation with subject matter experts, examination of relevant public and private-programs, examination of vendor marketing materials, and extensive web-searches for incident management-related terms. We asked our advisory panel, and additional subject matter experts from the government, private sector, emergency response community and academia, to identify relevant research we could draw upon.

Overall we found little study of CIMS interoperability in the public domain. In total, we collected 60 relevant documents during our review. ISTS researchers collected documents from; government programs, emergency management product vendors, standards bodies, policy organizations, academia, media, and military. A mixture of online research and personal contacts were used to collect the relevant documents. A bibliography of key reports identified during the literature review is found on page 28.

### **3. Vendor Survey**

#### ***Purpose, Objectives, and Scope***

The purpose of the vendor survey was to collect data on the status of interoperability between available CIMS programs by obtaining vendors' perspectives. Qualitative and quantitative data was collected through an online survey and during structured telephone interviews with vendors. The objectives of the survey were three-fold. The first objective was to assess data-sharing capabilities within CIMS solutions, with other CIMS solutions, and with non-CIMS solutions. The second objective was to determine if common structural design existed between CIMS (e.g., software features, data storage, data transfer). The third objective was to understand compliance with existing standards and extent of involvement with standards development organizations.

The scope of the survey was driven primarily by CIMS characteristics. As per our definition, the CIMS program had to be specifically designed to support the incident or

event information management functions for federal, state, and local emergency management organizations to be included in the survey. The program also had to be currently commercially available.<sup>6</sup> We did not include any prototype or in development software in the survey. Six subject matters reviewed the survey and it was piloted with nine people prior to administration via the web.

### ***Qualitative Interviews and Quantitative Survey***

The following actions were taken in order to ensure maximum vendor participation in the survey:

- All vendors included in the 2002 National Institute of Justice, Special Report: Crisis information Management Software (CIMS) Feature Comparison Report whose companies were still viable were invited to take part in the survey.
- A “call for vendors” advertisement appeared in Washington Technology’s WT Newswatch E-newsletter on August 2nd and 16th, 2004. The WT Newswatch e-letter is circulated three times per week to 40,000 subscribers.
- A request for participation was sent to the International Association of Emergency Managers Listserv. This resource provides a community discussion environment for emergency managers to share views, questions, and answers on emergency management issues.
- The Emergency Interoperability Consortium (EIC) distributed our request for participation in the vendor survey to all members of the consortium. The consortium now includes more than 60 private companies, public agencies, non-profit organizations and university groups.

Invitations to partake in the survey were sent to 42 vendors. Seventeen vendors completed the survey (response rate of 40%).<sup>7</sup> Two email follow-ups were conducted at ten-day intervals with vendors who had not yet completed the survey. Nine vendors completed two-hour, semi-structured, one-on-one interviews. All survey respondents who started the survey completed it.

## **4. Practitioner Workshop**

The purpose of the CIMS Interoperability Workshop was to capture and quantify the emergency management community’s assessment of the interoperability of existing CIMS platforms. On September 17, 2004 nine subject matter experts representing a cross

---

<sup>6</sup> In this context, ‘commercially available’ is meant to signify a product that can be readily implemented today—as noted by the qualifier of ‘no prototype software.’ Commercially available was not meant to exclude government sponsored or government-off-the-shelf (GOTS) products; in fact, extra strides were taken by the research team to include government sponsored and GOTS products in both the survey and final analysis.

<sup>7</sup> Survey conducted using online survey tool Zoomerang <<http://www.zoomerang.com>>. Two vendors completed the survey after final preparations were made for the workshop. Their responses were not discussed at the workshop; however, they are represented in the charts, figures and analysis presented in this report.

section of the emergency response community met on the campus of Dartmouth College to discuss the results of the literature review, and the interoperability research conducted to date, including the vendor survey. The results of the survey were presented to the workshop along with supporting data from the interviews and literature review. The ISTS team led a facilitated discussion and captured data through a networked decision support system that allows for anonymous real time collaboration between workshop participants.<sup>8</sup>

## **5. Data Analysis and Report Production**

Following the workshop the research team compiled the body of data collected and performed analysis. We grouped analytical conclusion into topic areas and provided a draft version of the report to both the advisory panel and workshop participants. Viewpoints of vendors, policy groups, government officials, and practitioners have all been considered in this study.

---

<sup>8</sup> GroupSystems decision support software is licensed through the Ventana Corporation.

## **FINDINGS AND ANALYSIS**

It is unclear how broadly CIMS are adopted across America. We found no statistics on CIMS adoption by organizations in the public or private sector. Larger population areas seem to be more likely to have adopted CIMS. For example, the City of Los Angeles helped a vendor develop one of the very first CIMS based on the City's needs. The Port Authority of New York / New Jersey has one of the nations most advanced implementations of CIMS and is pursuing novel approaches going beyond traditional CIMS applications themselves and seeking to enhance the incident command (IC) productivity, not reduce or burden the efforts of the IC. Specialization of products to sectors was not generally found. In fact, for the most part vendors told us that their products are designed for all hazard response. We discovered that a variety of products have been adopted by organizations to fit their particular needs. The unique federal system of government in America, with the resulting local autonomy, allows greater flexibility in individual CIMS purchase decisions. We found that larger population areas are pursuing forms of regionalized information and resource sharing.

The issue of interoperability between emergency management and disaster mitigation organizations is larger than just the CIMS component. Many systems provide a plethora of Command, Control, and Communications (C3) information that extends use of CIMS. Such programs would include Geographic Information Systems (GIS), weather and plume modeling, aerial photography, street mapping, and real time closed-circuit television data. We acknowledge here that examining the breadth of issues surrounding interoperability between all levels of C3 software is well beyond the scope of this report.

We found no published documents specifically focused on CIMS interoperability. Related materials we collected addressed CIMS interoperability as a component of larger studies. From our literature review we drew the following conclusions. First, emergency management data interoperability is a national imperative. Several expert commissions and government reports noted that a key element of our national preparedness is the ability of our first responders to have the most advanced tools at their disposal for situational awareness. Second, there are a number of organizations working on standards; however, we found that overall coordination efforts are lacking. Third, we found no common published vocabulary that is universally accepted by the emergency management community. We discuss elements of these conclusions in the following passages.

### **CIMS Definitions and Terminology**

***Our research indicates there are a range of functional areas that should be included in future definitions of CIMS***

The 2001 *Crisis Information Management Software (CIMS) Feature Comparison Report* defined conditions to identify CIMS products serving the information management needs of State and local emergency management agencies. Specifically the product needed to be designed to support crisis or event information management functions of state and

and/or local emergency management organizations and the product was commercially available (no 'beta' version software was considered).

During our research, we developed a revised definition of CIMS use and functionality. We defined CIMS as programs specifically designed to support incident or event information management functions for federal, state, and/or local emergency management. Practitioners we interacted with on this research project told us that CIMS are larger than just the software in use in Emergency Operations Centers (EOCs); CIMS actually facilitate a wide range of functions from day-to-day management to planning to event and incident response. Participants in this research effort indicated that including specific functionality may improve future CIMS definitions.

In our literature review, we found that the Organization for the Advancement of Structured Information Standards Emergency Management Technical Committee (OASIS EM TC) charter outlines functions that are useful for future CIMS definitions<sup>9</sup>. The functions identified by the OASIS EM TC charter:

- Asset and resource management
- Emergency GIS data accessibility, interfacing, and/or usage
- Monitoring and data acquisition systems (CBRN sensors, cameras, etc)
- Notification methods and messages
- Source tasking
- Situation reporting
- Staff, personnel, and organizational management

In addition, our research indicates that these following functional areas should be considered for inclusion in subsequent definitions.

- On scene situational awareness
- Preparedness, planning and training
- Accounting and Reimbursement (part of asset and resource management)
- Data mining and analysis
- Security management (access/authentication/verification)

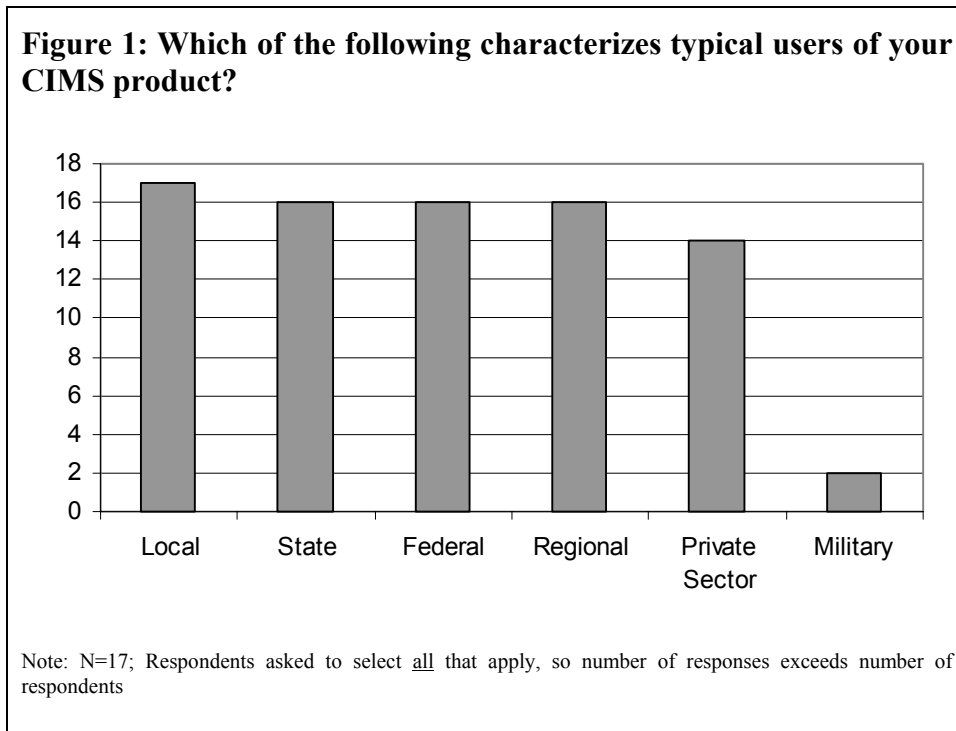
***Future CIMS definitions should be expanded to include other critical infrastructure sectors***

Our research indicates that CIMS are in use by all levels of government and private industry across many sectors. When asked, "Which of the following characterizes typical

---

<sup>9</sup> OASIS is a not-for-profit, international consortium that drives the development, convergence, and adoption of e-business standards, for more information, please see URL <[http://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=emergency](http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=emergency)>

users of your CIMS product?” federal, state, regional, local, and private sector clients were all represented strongly (Figure 1).



The survey data was validated during the practitioner workshop. Our participants indicated that CIMS are in use beyond the federal, state and local emergency management agencies, including the following:

- Private sector including infrastructure companies such as telecommunications, utilities, and security
- Health care industry
- Volunteer organizations / non-profits
- Educational organizations

One participant noted that public private partnerships are becoming increasingly important to CIMS data acquisition.

If CIMS is defined generically as being inclusive of incidents or events regardless of sector, then by definition, it should be inclusive of all sectors. If it is restricted to EOC's for public safety agencies only, then it is capturing only a subsegment of the universe where emergencies and/or events originate and get managed. Within sectors like healthcare, transportation, energy, telecommunications agriculture, banking, incidents/events occur all the time and are managed by various systems. In addition, the data captured by these discrete systems may become contextually highly relevant to the public safety EOC's.

Overall we note that CIMS adoption and use involves the coordination of many disciplines. Information must be mapped across communities and sectors. Less

sophisticated partners need to be able deliver information to, and obtain information from, the more sophisticated users' CIMS. Stakeholders want and need control over the flow of information. Some participants noted that it seems like emergency response community is "catching up" to other critical infrastructures since it has not adopted broad standards for information sharing. Others noted that the emergency response community should follow the examples of the financial services and consumer products industries. These industries use a common taxonomy and establish standards for the exchange of a wide array of information elements.

***There is no broadly accepted vocabulary of technical terms for use with CIMS***

At this time, there is no broadly accepted vocabulary of technical terms for use with CIMS. Without such a terminology members of the community including practitioners, vendors, and academics will continue to struggle in all levels of interoperability development. We found that published glossaries often cover only those materials pertinent to the author's report. In other areas, strides have been made to address components of the overall lexicon, e.g. the titles, duties and command structure of a personnel responding to an incident as defined in the Incident Command System; but incomplete acceptance within the community continues to stifle cooperation as well as additional efforts to develop a common language and response posture.

One workshop participant noted, "Half the battle is to have a common language – we don't even know each others' language and acronyms. LA has so many incidents that they do talk same language and it's easier, whereas NYC doesn't. If you can't even get a common thread among emergency management, how can you get the emergency management data shared?" Both vendors and practitioners expressed frustration with the lack of a common lexicon. Without common terminology it is difficult to exchange data broadly. The way one CIMS program classifies a fire truck, for example, may be completely different than another CIMS systems at this time. Without some level of lexicon, resource typing, common language, etc. each instance of interoperability is and will continue to be a specific effort of mapping one groups 'variables' against another groups set of variables. Practitioners we spoke with expressed the need for efforts to determine what information or "data elements" needs to be exchanged across jurisdictions and disciplines. A consensus-driven needs document may serve as a starting point for common terminology relevant to CIMS emergency incident management and response.

## **CIMS Interoperability**

### ***Background***

Our literature review revealed few documents examining CIMS interoperability. One of the only documents to directly address this issue is the *Crisis Information Management Software (CIMS) Feature Comparison Report*. The authors reported that there was no significant effort underway for standardization in the different software products in 2001. Further, the report finds that the automated exchange of information between agencies using different products will continue to be problematic without intervening efforts to develop and promulgate standards. Our research indicates that since the *Feature Comparison Report* was published government efforts, standards bodies, vendors, the user community and various interdisciplinary consortia are working to move interoperability forward. Yet significant challenges remain. In the following passages, we outline non-government, government, and vendors efforts relating to interoperability.

### ***Non-governmental efforts—including standards organizations—are working to promote the interoperability of CIMS***

Our research indicates that there are a number of efforts underway that may assist the interoperability of CIMS. Strategic reports, methodologies, and standards are being produced by non governmental organizations. An example of a strategic document examining responder information sharing is the report titled *Creating A Trusted Information Network for Homeland Security* from the Markle Task Force on National Security.<sup>10</sup> The report provides some detail on a “proposed System-wide Homeland Analysis and Resource Exchange (SHARE) Network” that may include CIMS type systems.

We discovered the existence of several relevant standards during our research. For example OASIS developed and published the Common Alerting Protocol (CAP) with the backing of an association of emergency response software vendors called the Emergency Interoperability Consortium.<sup>11</sup> The CAP “is a simple but general format for exchanging all-hazard emergency alerts and public warnings over all kinds of networks.”<sup>12</sup> The Institute of Electrical and Electronics Engineers (IEEE) has developed a relevant standard called IEEE1512.<sup>13</sup> In addition, relevant work is ongoing through the Office of Justice Programs (OJP) and the Global Justice Information Sharing Initiative (Global).<sup>14</sup> Recently a group called the Emergency Data Exchange Language (EXDL) working

---

<sup>10</sup> See URL <[http://www.markle.org/markle\\_programs/policy\\_for\\_a\\_networked\\_society/national\\_security/projects/taskforce\\_national\\_security.php#report1](http://www.markle.org/markle_programs/policy_for_a_networked_society/national_security/projects/taskforce_national_security.php#report1)>.

<sup>11</sup> More information on the EIC, OASIS and the Common Alerting Protocol can be found at the following URLs <[http://www.oasis-open.org/news/oasis\\_news\\_05\\_05\\_04.php](http://www.oasis-open.org/news/oasis_news_05_05_04.php)> and <<http://www.eic.org>>.

<sup>12</sup> More information is available at URL <[http://www.partnershipforpublicwarning.org/ppw/docs/cap\\_press.pdf](http://www.partnershipforpublicwarning.org/ppw/docs/cap_press.pdf)>.

<sup>13</sup> More information is available at URL <<http://grouper.ieee.org/groups/scc32/imwg/>>.

<sup>14</sup> More information is available at URL <<http://it.ojp.gov/index.jsp>>.

group developed a common SOAP XML header for the EXDL messages.<sup>15</sup> This effort may prove a significant step forward by providing a common ‘envelope’ for messages to be sent and received within disparate systems.

Other efforts are underway as well. The Communications for Coordinated Assistance and Response to Emergencies (ComCARE Alliance) is a “broad-based, not-for-profit national coalition of more than 95 organizations representing nurses, physicians, emergency medical technicians, 9-1-1 directors, emergency managers, transportation officials, wireless, technology and transportation companies, public safety and health officials, law enforcement, automotive companies, consumer organizations, telematics suppliers, safety groups, and others.” Its mission is to “encourage the development and deployment of communications and information technologies that will enhance America's emergency capabilities and facilitate cooperation across professional, jurisdictional and geographic lines, seeking to break down the walls that separate these agencies, businesses and professions, and thus limit their effectiveness.”<sup>16</sup> The Multi-sector Crisis Management Consortium has a mission to “develop and deploy new IT strategies, architectures and tools to support crisis management and emergency response communities.”<sup>17</sup> Another effort, the Partnership for Public Warning is committed to “promote and enhance efficient, effective, and integrated dissemination of public warnings and related information so as to save lives, reduce disaster losses and speed recovery.”<sup>18</sup> These organizations provide forums for CIMS related coordination on interoperability.

### ***Government efforts are underway to promote the interoperability of CIMS***

Communications interoperability requires the coordinated efforts of leadership at the local, state, and federal levels. While most users believe agencies within state governments have stepped forward, they are looking for more emphasis on Federal and interstate coordination. Both federal coordination efforts and actual software tools are available from government entities. HSPD5 Calls for the development of a National Response Plan and a National Incident Management System and lays out the responsibilities of Federal Agencies and the corresponding Assistants to the President.<sup>19</sup> Government coordination efforts include the Department of Homeland Security Office of Interoperability and Compatibility. A component of the Science & Technology directorate the OIC will “oversee the wide range of public safety interoperability

---

<sup>15</sup> More information is available at URL <[http://www.oasis-open.org/committees/download.php/9156/EDXL\\_StdMsg\\_draft-8-23-04\\_1.doc](http://www.oasis-open.org/committees/download.php/9156/EDXL_StdMsg_draft-8-23-04_1.doc)>.

<sup>16</sup> Further information on the COMCare Alliance is available at URL <<http://www.comcare.org/>>.

<sup>17</sup> Data on the MSCMC is available at their website, URL <<http://www.mscomc.org/goals.html>>.

<sup>18</sup> “The Partnership for Public Warning is a non-profit, public-private partnership established in 2002 to save the lives and property of people at risk from natural disasters, accidents and terrorism by improving the nation’s alert and warning capabilities.” More information is available at URL <<http://www.partnershipforpublicwarning.org/ppw/>>.

<sup>19</sup> Homeland Security Presidential Directive 5 (HSPD5) - Management of Domestic Incidents, published by the Office of the President, February 28, 2003, available at URL <<http://www.whitehouse.gov/news/releases/2003/02/20030228-9.html>>.

programs and efforts currently spread across Homeland Security” including “interoperability issues relating to public safety and emergency response.”<sup>20</sup> The OIC is specifically charged with supporting the creation of interoperability standards, establishing a comprehensive research, development, testing, and evaluation (RDT&E) program for improving public safety interoperability, conducting pilot demonstrations, creating an interagency interoperability coordination council, and working with the National Incident Management System (NIMS) Integration Center. The NIMS Integration Center (NIC) has been set up to provide strategic direction and oversight of the NIMS. DHS reports that the NIC will “develop and facilitate national standards for NIMS education and training, first responder communications and equipment, typing of resources, qualification and credentialing of incident management and responder personnel, and standardization of equipment maintenance and resources.” We believe that overall coordination of CIMS efforts is critical. However, our assessment of government coordination efforts is incomplete. We were not able to ascertain the status or success of government efforts since at the time of our study the relevant efforts were just beginning to ramp up.

Government entities also provide some CIMS type software systems. For example the Disaster Management Interoperability Services (DMIS) program is “providing new software tools at no cost to responder organizations for increased disaster response effectiveness” and is dedicated to “improving disaster response by enabling responders to share information seamlessly between organizations.”<sup>21</sup> DMIS has made available software tools at no cost to responder organizations and employs a SOAP-XML and Web Services Definition Language (WSDL) for interoperability. The Disaster Management Initiative (DMI) uses DMIS software and provides an Internet-based portal that may serve to “improve the delivery of disaster assistance information and services.” The DMI provides disaster information and situational awareness tools including a national map, weather updates, web mapping services, and may handle specific requests. The National Fire Incident Reporting System (NFIRS 5.0) is CIMS package for fire departments.<sup>22</sup> The package allows departments to “report and maintain computerized records of fires and other fire department incidents in a uniform manner.” The tool set was developed by the United States Fire Administration (USFA) in partnership with the National Fire Information Council (NFIC). The National Interagency Resource Ordering and Status System (ROSS) project is another government effort in CIMS. Sponsored by the National Wildfire Coordinating Group (NWCG), ROSS is a computer software program which automates the resource ordering, status, and reporting process and tracks all tactical, logistical, service and support resources mobilized by the incident dispatch community.<sup>23</sup>

---

<sup>20</sup> More information is available at URL <<http://www.dhs.gov/dhspublic/display?content=4044>>.

<sup>21</sup> More information is available at URL <[http://www.cmi-services.org/dmishp\\_what\\_is\\_dmis.html](http://www.cmi-services.org/dmishp_what_is_dmis.html)>.

<sup>22</sup> More information is available at URL <<http://www.nfirs.fema.gov/>>.

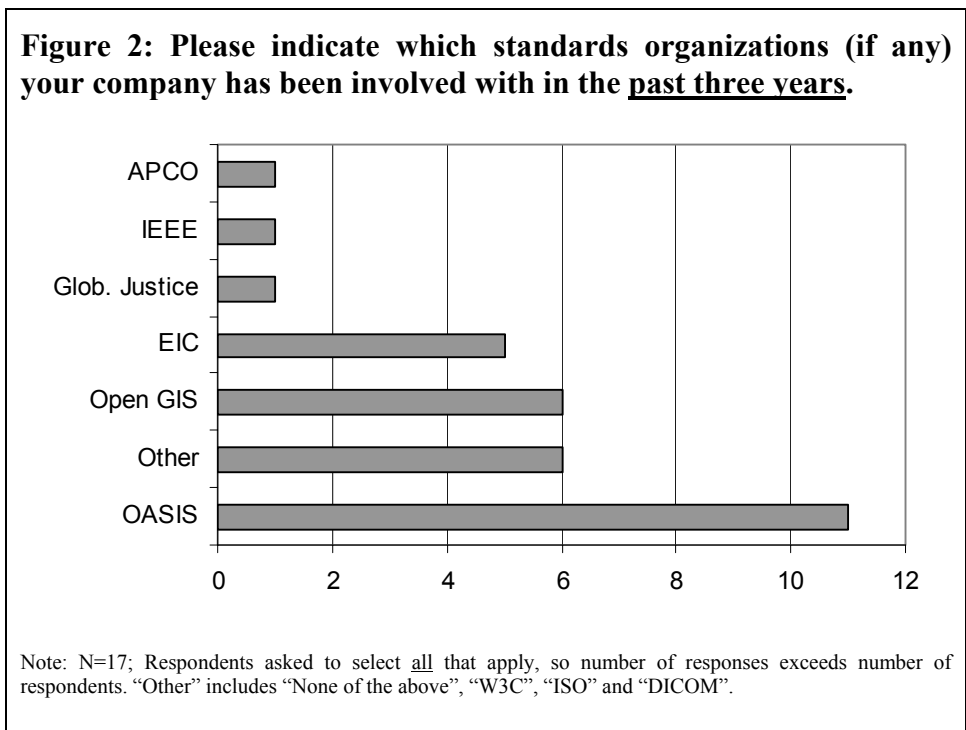
<sup>23</sup> Established in 1997 and chartered by the NWCG in June 1998, the scope of ROSS focuses on automating current processes enabling dispatch offices to electronically exchange and track information near real-time. More information is available at URL <<http://ross.nwcg.gov/>>.

Overall we believe that current government efforts provide a starting point for broader CIMS interoperability. The parties in our study believe that the adoption of current methods and standards by practitioners and vendors alike will increase CIMS interoperability. We estimate that, from practitioner’s standpoint, the government’s assignment of responsibilities regarding interoperability has neither helped nor hindered efforts to increase CIMS interoperability to date. At this time, the government’s efforts are ongoing and time is needed to see what affect they have on CIMS interoperability.

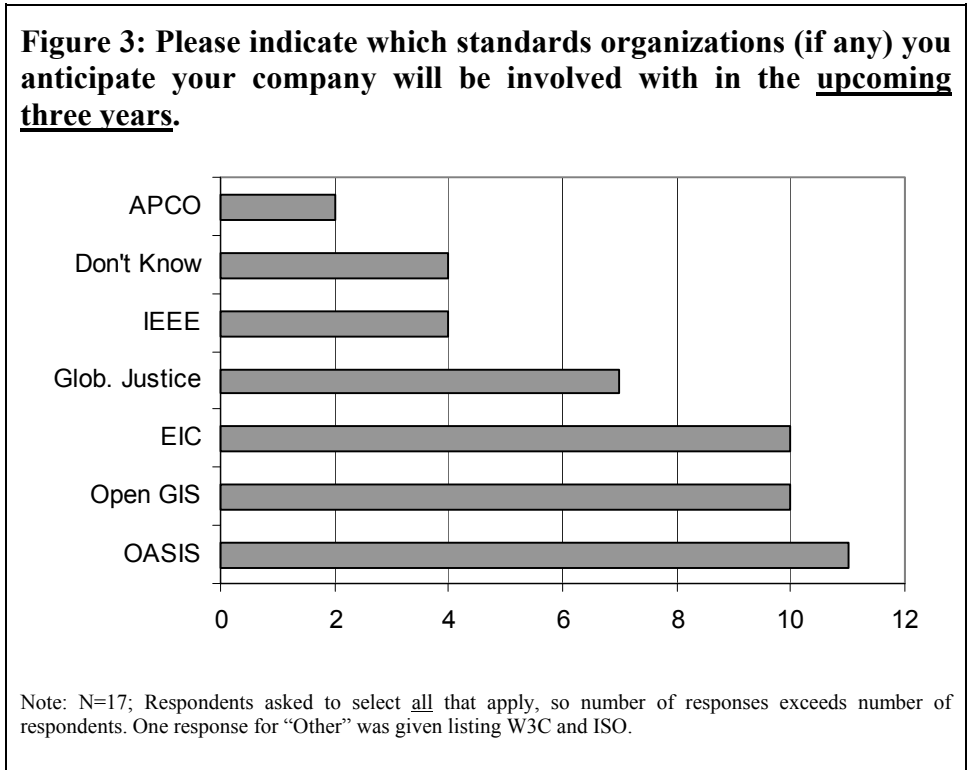
The participants did note that government efforts may take longer to develop and may be less responsive to community needs than private sector developments. To address timeliness and responsiveness both practitioners and vendors advocated the use of public private partnerships to drive government sponsored or sanctioned standards efforts. The consensus of our research subjects is that government efforts must be relevant to make a difference. By bringing parties involved together and developing a framework for CIMS interoperability the government may facilitate rapid developments toward better situational awareness capabilities for emergency managers.

***Vendor efforts are underway to enhance interoperability***

Our survey indicates that vendors are involved in standards organizations and various consortia dedicated to improving CIMS interoperability. When asked, “which standards organizations (if any) your company has been involved with the past three years that is, since 2001” most vendors indicated that they had been involved with at least one standards organization—in fact 65% of the vendors surveyed stated they have been involved with OASIS within the last three years (Figure 2).



Further the majority of the vendors that participated in our survey indicate that they anticipate their company will be involved with additional standards bodies in upcoming three years (Figure 3, Page 18).

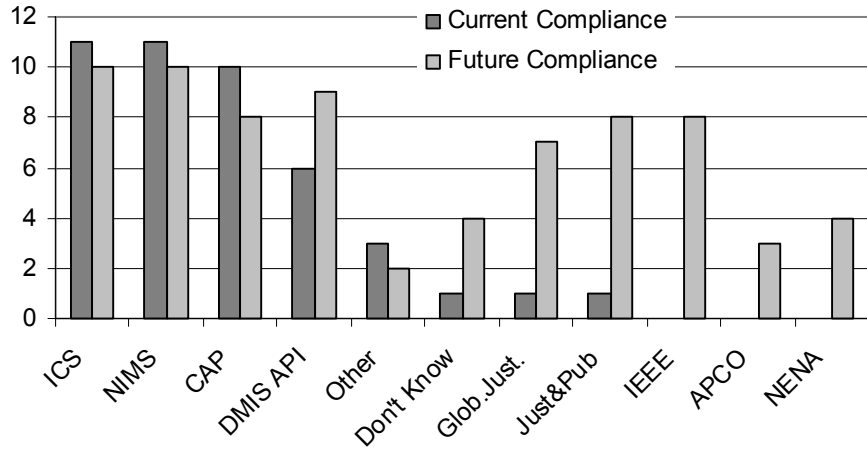


Most vendors are ensuring products meet current and developing industry methodologies and standards. For example the majority of the vendors surveyed indicated that they are currently compliant with the Incident Command System (ICS), National Incident Management System (NIMS), and Common Alerting Protocol (CAP). In addition vendors plan to be compliant with a growing number of industry methodologies and standards in the next three years (Figure 4, Page 19). Lastly our structured interviews with vendors indicated that some vendors are participating in CIMS interoperability demonstrations.

From a vendor perspective CIMS are both relatively interoperable and intraoperable. All of the vendors (100%) in our survey told us that computers or servers within their CIMS program can share data with each other. The most common method of data transfer used to share data within CIMS programs in our survey is the Internet Protocol (IP) (Figure 5, Page 19).<sup>24</sup> The majority of the vendors that responded to our survey, 82%, said that their CIMS program shares data with other CIMS programs (Figure 6, Page 19). The eXtensible Markup Language or XML is the most common language for the interchange of structured data found in our survey. The majority of the vendors in our survey used

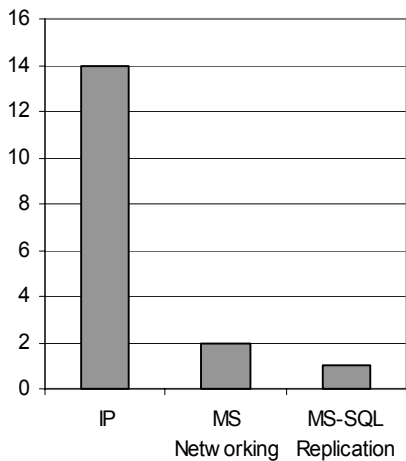
<sup>24</sup> IP is an abbreviation for Internet Protocol, an agreed upon format for transmitting data between devices.

**Figure 4: Please indicate which standards organizations (if any) you anticipate your company is currently involved and will be involved with in upcoming three years.**



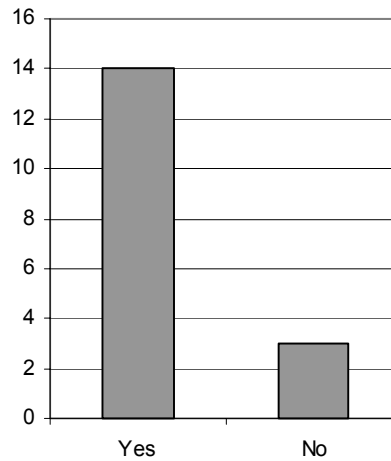
Note: N=17; Respondents asked to select all that apply, so number of responses exceeds number of respondents. "Other" includes "Open GIS", "HAN", "PHIN", "EM XML"

**Figure 5: What is the method of data transfer used to share data within your CIMS programs?**



Note: N=17; Respondents asked to select all that apply, so number of responses exceeds number of respondents

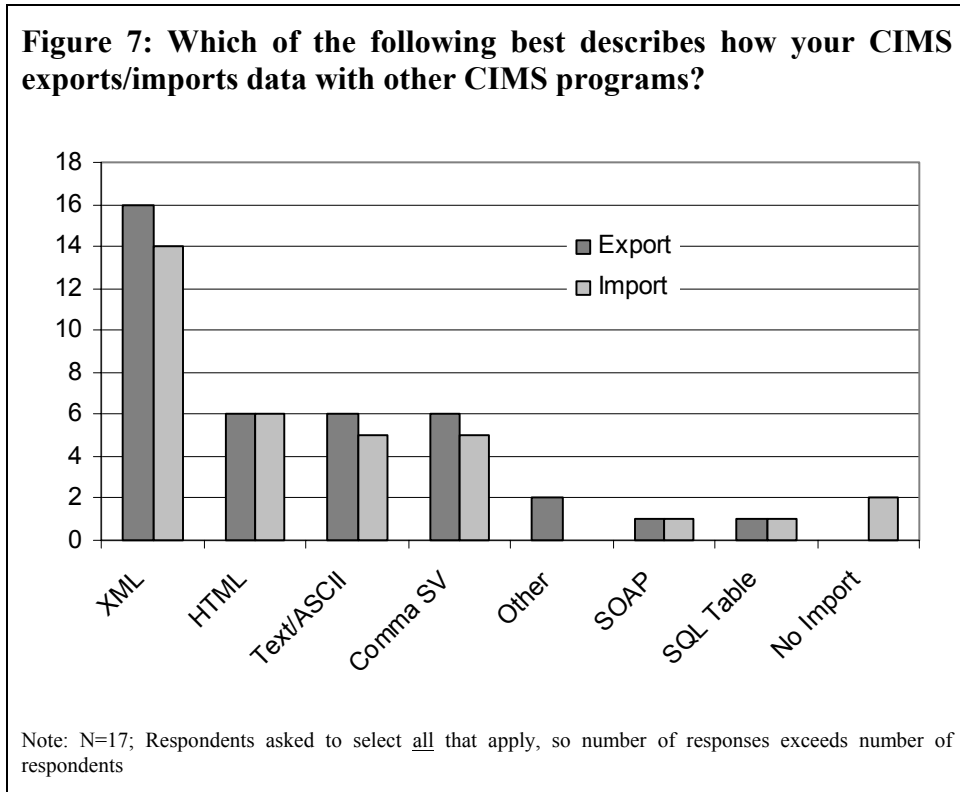
**Figure 6: Does your CIMS program share data with other CIMS programs?**



Note: N=17; Respondents asked to select all that apply, so number of responses exceeds number of respondents

XML for both data import and export (Figure 7, Page 20).

Vendor responses in our survey indicated that all CIMS use databases to store data. This led us to ask the question “Is the interoperability of CIMS really a database integration issue?” The practitioners in our study commented that if CIMS interoperability was simply a data fusion issue it would have been solved already. We believe that the survey data supports this position. The majority of vendors can share data using XML; however, problems remain.



## **Interoperability Challenges**

### ***Background***

As we outlined in the preceding passages, since 2001 significant progress has been made by non-government, government, and vendors to improve the ability of CIMS to share data. Yet with all of these efforts underway the practitioners we worked with on this study told us that there are significant challenges ahead. For example, will certain methodologies and standards be pushed by government or will non-government standards bodies be able to take the lead on CIMS interoperability? One practitioner related that “many government agencies...recognize the need for data interoperability, but unfortunately efforts seem to reinforce the stovepipe mentality that currently exists rather than promote communications across the stovepipes.” Others noted that government has been slow to take a leadership role in the development of standards. Lastly, vendors are reporting that they are working towards complying with multiple standards from different

organizations since no single guide exists. These are by no means the only challenges. In the following passages, we outline a number of additional interoperability challenges in the CIMS domain that we identified during this study.

### ***Information technology adoption and planning issues in the emergency management community***

The practitioners involved in this study related that many emergency response organizations simply do not use CIMS. Possible reasons we identified from our structured interviews with emergency managers and practitioner workshop are 1) cultural resistance to adopting Information Technologies (IT), 2) lack of IT resources, 3) information technologies may not be considered in planning processes or is not a priority equipment purchase.

During our research we heard from our practitioners that, within the emergency management and response communities, certain sectors are very resistant to change. Relevant to our study, our experts reported that in their experience the adoption of information technologies in operational and response capacity is not uniform across the sector. Some responders maintain a sentiment that ‘if it ain't broke don't fix it’. Much of the emergency response community is able to manage incidents events without the automated information management systems. One workshop participant stated that it was not the everyday events where IT would be needed, but the events where local, and even perhaps regional, resources would be exhausted, necessitating a need for a greater level of coordination between agencies that may not be familiar with one another.

Further, the participants in our survey related that they believe that the emergency management community as a whole has not fully embraced the use of information technology as a communication tool. One participant noted that organizations are still “...grappling with voice/radio issues and have yet to embark on the information side.” Voice is seen as the primary data exchange medium and data as a secondary, static, repository. Another participant noted that it is fair to say that the biggest challenge to achieving large scale data interoperability is to get emergency management organizations to actually start using data tools as opposed to relying on point to point (mostly voice) communications for situational awareness.

In smaller communities, emergency responders may not have the IT resources to support CIMS. Even if IT resources are available some communities may lack the technical support needed to employ CIMS. This means that first responders do not have the benefit of the situational awareness that CIMS provide. One of our workshop participants commented:

Lack of technology impacts emergency management. A lot of institutions don't even have email and access to an internet, or a firewall, so they certainly can't move to the next step of collaboration. In the revolution of info sharing in EM, there have been a few revolutions. It started with a bell, then radios and a telephone about 100 years ago. They're not going away, but are point-to-point so limited by scale. Then came CNN. CIMS is a higher level – data sharing (not just voice) in a collaborative environment. So move from synchronous, point to point to asynchronous many to many. One of challenges with this is the diversity in sophistication: some tiny jurisdictions are very sophisticated and using systems internally to facilitate business processes and yet other large federal organizations are really basic.

In some response organizations, IT resources are not a priority equipment purchase. IT resources are often viewed as a component of the administrative functions of an organization, and not an integral part of the incident management. Our participants noted that in their experience IT resources are not often considered when planning for the next year, or even the coming five years. When facing limited annual resources, upgrading physical equipment is often a higher priority than their IT infrastructure. This is compounded at the first responder level by the need to keep their equipment up-to-date with evolving safety codes. As difficult as it may be to keep equipment up-to-date and functional, it can be more daunting for organizations to keep their computer systems current, secure and functioning properly. Outside consultants are often needed to manage their IT resources. These factors also make it difficult to forecast the money needed to sustain an organization's IT infrastructure over the long term; particularly if the person who is responsible for planning and budgeting is not familiar with what is required to keep the IT infrastructure running properly. Our participants felt that these factors directly affect the ability for responder organizations to support the implementation of CIMS.

### ***Social obstacles to information sharing***

We have noted in preceding passages that there are both adoption and planning impediments to interoperability. Our participants also reported cases when interoperability and information sharing capabilities were established over secure lines for incident management and yet little data was shared. Why did this occur?

The participants were asked to comment on these cases. Participants noted that there are "cultural issues" that affect information sharing. When incidents occur, information is often shared through informal back channels such as phone calls and emailed documents. Our practitioners commented that in some circumstances, individuals do not want to lose control over their information. Information owners want to control who sees data and who users can send their data to. Our workshop participants noted that sending sensitive information to someone you do not personally know, regardless of the security of the transmission medium itself, was not something they saw occur.

We believe that training and simulations are appropriate tools to address cultural information sharing issues. This is supported by the experiences of our study's participants. They informed us that in order to develop trusted relationships, it is valuable to "game out" situations they may encounter in real life. Our study participants articulated that cross-sector exercises (including participants from all critical infrastructures) should be an ongoing national priority. Cross-sector exercises may be particularly useful for determining where choke points in information sharing exist. One participant noted that organizations often look for interoperability within their own discipline, e.g., hospitals look within hospitals; this results in blind spots that may become readily apparent when an incident occurs.

### **Recommendations to Move Interoperability Forward**

In the preceding sections of this document, we have focused on the current status and challenges regarding CIMS interoperability. In the following passages, we provide

recommendations to move CIMS interoperability forward. Our recommendations are based on the entire body of the data collected during this study. We provide the following recommendations:

1. Establish a practitioner working group to develop a CIMS terminology and consensus-driven, user-defined needs
2. Coordinate standards efforts across critical infrastructure sectors
3. Develop incentives to encourage vendor compliance with standards as a key driver towards CIMS interoperability
4. Interoperability needs to be a priority in the CIMS purchase process
5. Develop purchasing guidelines
6. Promote CIMS interoperability goals in exercises and create a repository for lessons learned
7. Initiate research into data security, including permissions and trust, in CIMS interoperability

***Establish a practitioner working group to develop a CIMS terminology and consensus-driven, user-defined needs***

The 2001 *Feature Comparison Report* calls for users to drive interoperability solutions. The report's authors write; "The solution to this problem lies only partly with the industry. The larger share of this responsibility belongs to the user community to establish standards and insist on products that meet this important requirement."<sup>25</sup> The practitioners we collected data from generally agreed. One participant wrote that "the user community should not adjust to the available vendor solutions/technology available. The user community should be influencing what is the technology available." However, some data indicates that there may be a disconnect between the user and vendor communities.

For example, one vendor representative in our survey wrote "...we have been hearing the user community calls for interoperability; that same community has not been able to articulate what is the problem that is being resolved through interoperability. It appears that most of the requirements are being driven and outlined by the vendors, rather than the end users." One of our workshop practitioners supported this position by noting "The user community is still so fragmented that it is difficult to bring them together to develop a common taxonomy, standards and protocols. For example, ask a number of different stakeholder groups what the definition of interoperability is and you will get a variety of different answers. So if the user community cannot agree on what it is, how can the vendors respond to the requirement?" Although the *Feature Comparison Report* and the vendor community both expressed the need for a greater level of user involvement in standards and interoperability work, we found no group of CIMS users that could speak on behalf of the larger user community.

---

<sup>25</sup> *CIMS Feature Comparison Report*, URL <<http://www.ojp.usdoj.gov/nij/pubs-sum/197065.htm>>.

Based on the research we conducted, we conclude that a practitioner working group with the goals of developing a CIMS terminology and consensus-driven, user-defined needs is a missing component of the framework needed to facilitate change nationally. Throughout our research, members of the vendor and standards community both expressed that greater clarification on the user's needs regarding interoperability is required. As one of our workshop participants noted, "We need to be able to share base fields that are critical. Requirements analysis is key more specific or granular data elements derived from the end user community." This is particularly required in light of new national imperatives such as the National Incident Management System. Without clear definitions of the roles of responders and clear delineations placed on the information flow, it is difficult to memorialize the management of incidents and events into software code.

### ***Coordinate standards efforts across critical infrastructure sectors***

The participants in our study told us that future definitions of CIMS need to be expanded to include other user groups across critical infrastructure sectors. We note here that many of the standards efforts that are underway are standards efforts sector specific yet overlap into other critical infrastructure sectors. The consensus of our study participants is that it is in the best interest of the responder community as a whole to coordinate standards efforts to limit redundancy and to maximize the vendor's standards compliance efforts. The Department of Homeland Security has the mandate to undertake this effort. As one of our participants noted, "Although the CIMS challenges can be addressed in the trenches, the information sharing protocols needs to start at the top, DHS." We encourage DHS to move quickly to address this national need.

### ***Develop incentives to encourage vendor compliance with standards as a key driver towards CIMS interoperability***

Practitioners and vendors alike told us that market demand will drive the features found in CIMS. Standards often play a role in market demand since they are expressions of the user communities needs. In the current environment, many standards exist with overlapping criteria. We believe multiple overlapping standards complicate vendor compliance and CIMS interoperability overall.

If parties involved in CIMS development and use can work with government to develop a common set of standards across critical infrastructure sectors then incentives can be developed to drive interoperability. For example, if data exchange structures were defined and sanctioned by the Federal, government grant monies could be tied to their implementation. Vendors and practitioners alike would benefit by having a common base to build upon when purchasing, implementing, and maintaining CIMS.

### ***Interoperability needs to be a priority in the CIMS purchase process***

As we noted in our discussion of incentives for vendor compliance, one benefit of having broadly accepted standards is the ability of the user community to integrate them into their purchasing process. At this time, users told us that interoperability is often a low priority compared to other imperatives when purchasing CIMS. We believe that it is

critical for organizations that purchase CIMS to consider the interoperability needs of your regional partners when selecting a CIMS program.

Throughout our research, we have encountered CIMS users that placed interoperability low on their list of requirements. Once the systems became operational, data sharing needs quickly moved to the forefront of users' requirements. We encourage prospective CIMS purchasers and those upgrading their systems to place a greater relative priority on interoperability during their requirements analysis. We believe that without this change in thinking, a general lack of interoperability will continue to cascade across CIMS implementations.

### ***Develop purchasing guidelines***

In order to help organizations integrate interoperability thinking into their purchase or upgrade processes, we provide the following guidelines regarding CIMS interoperability to assist organizations when building purchasing requirements:

- Any product or service offered as part of CIMS procurement must be demonstrably compliant with relevant, published, validated and commercially supported interoperability standards including CAP, and IEEE 1512 for example.
- Products and services offered must have the ability to operate within established operational methods including, for example, ICS and NIMS.
- In addition, it is further expected that products or services may be obliged in the future to also be compliant with published, validated and commercially supported interoperability standards drawn from other disciplines (healthcare, electronic banking, security, etc.).
- The CIMS should have the ability to import/export data, preferably on a real-time basis, in an accepted data exchange format such as XML, SOAP XML, etc.

### ***Promote CIMS interoperability goals in exercises and create a repository for lessons learned***

As we wrote in preceding passages, during our research we discovered that there were situations where the technical ability to share information securely existed, but information was not shared due to social and cultural factors. We believe one of the most effective ways to combat this dilemma is through exercises. The parties involved in this study agree. Exercises provide a common frame work for groups to test and improve their capability to respond to emergency incidents. We recommend that national exercises such the Top Officials (TOPOFF) series include the testing and evaluation of CIMS interoperability related issues.<sup>26</sup>

Including CIMS specific tests and goals will be a critical first step; however, other components are needed to ensure that the lessons learned are made available to the people when need them. We support our study participants' position that a national repository of

---

<sup>26</sup> More information is available at URL <<http://www.dhs.gov/dhspublic/display?content=735>>.

after action reports and lessons learned is created. Such a resource, to our knowledge, does not exist today. The creation of a one stop shop for CIMS related materials would significantly increase the ability of the critical infrastructure practitioners to develop their understanding of CIMS. The academic community has a key role to play here as well. We recommend that additional research be conducted as “case studies” into how into the development of information sharing policies can establish trusted sharing of data.

### ***Initiate research into data security, including permissions and trust, in CIMS interoperability***

When the technical problems regarding interoperability are removed, other problems become apparent. One of these problems is the issue of data security, including permissions and trust. If an interoperable system of systems is developed, a process for authenticating users, setting user access rights, rights of users to access materials and add other users must all be considered. As one of our study participants noted:

Data security is a big issue. If it is not solved, it will be very difficult to move forward. In various stakeholder advisory groups, these issues have been raised time and time again: (1) who has the ability to send incident messages; rights should be granted based on agency type and incident type (2) agencies need to classify data elements that can and cannot be shared (3) data viewing should be restricted based on need to know. For example, only certain responders should have the ability to view personal medical information which is often provided by telematics vendors at car crashes. (4) establish hierarchies so that only certain agency types can override what agencies should receive information.

Practitioners and vendors are all concerned about the security of their data. We recommend that research be conducted into the issue of permissions and trust before it becomes a limiting factor in interoperability.

## **ADVISORY PANEL MEMBERS**

Mr. Richard Andrews, Ph.D.  
Senior Director, Homeland Security  
National Center for Crisis and Continuity Coordination

Lieutenant Colonel Joey Booth  
Deputy Superintendent  
Crisis Response and Special Operations  
Louisiana State Police

Mr. Peter A. DeNutte, ENP  
Assistant Director  
New Hampshire Department of Safety  
Emergency Communications Section

Mr. Richard D. Jacques, Ph.D.  
Senior Program Manager  
Office for Domestic Preparedness  
Department of Homeland Security

Mr. Dan McGowan  
Administrator  
Disaster & Emergency Services Division  
Department of Military Affairs

Mr. John Paczkowski  
Director of Operations and Emergency Management  
The Port Authority of New York and New Jersey

Mr. James Schwartz  
Fire Chief  
County of Arlington, Virginia

## BIBLIOGRAPHY

The following reports were relevant to, and/or used in the creation of, this study.

Appel, Ed, Joint Council on Information Age Crime. *Technologies for Public Safety in Critical Incident Response*. Presentation. Office of Science and Technology, National Institute of Justice. September 23, 2003

Arlington County. *Arlington County Conference Report: Lessons Learned from 9-11 Attack on the Pentagon*, Arlington, VA: Arlington County, 2003

Avramov, Stoyan. *Integrating COTS Technologies into a Scalable Mobile Emergency Command Post*. Information & Security. Volume 10, 2003, pages 87-96

Barrouquere, Brett. *Technology Maps Hurricane's Effects*. Baton Rouge, LA: The Advocate, Capital City Press. September 19, 2003

Bell, Charlie and Scott Eyestone. *Disaster Management Interoperability Services (DMIS) at TOPOFF 2: Supporting Operations & Advancing Technology*, Interview. EIIP Virtual Forum, [www.emforum.org/pub/eiip/lc030521.txt](http://www.emforum.org/pub/eiip/lc030521.txt)

Botterell, Art ed. *Common Alerting Protocol, v. 1.0, OASIS Standard 200402*, OASIS Open EMTC, March 2004, [www.oasis-open.org/committees/emergency/](http://www.oasis-open.org/committees/emergency/)

Colvin, Butch. *Top Officials (TOPOFF) National Counter Terrorism Exercise Briefing*. Presentation. Department of Homeland Security. February 2004

Department of Homeland Security. *National Incident Management System*, Washington, D.C: Department of Homeland Security, March 1, 2004

Disaster Management Interoperability Services. *Introduction to Disaster Management Interoperability Services (DMIS)*, Web-based presentation. [http://www.cmi-services.org/includes/Intro%20to%20DMIS\\_files/frame.htm](http://www.cmi-services.org/includes/Intro%20to%20DMIS_files/frame.htm)

*E Team and ITspatial Form Strategic Alliance to Offer Integrated 3D GIS Mapping for Emergency Response and Incident Management Applications*. Press Release. Business Wire. February 6, 2003

Emergency Interoperability Consortium. *The Emergency Interoperability Consortium*. Point paper. Emergency Interoperability Consortium. [www.eteam.com/government/EICFinal.pdf](http://www.eteam.com/government/EICFinal.pdf)

Epper, Robert C., Mary J. Taylor, and Thomas K. Tolman. *Wireless Communications and Interoperability Among State and Local Law Enforcement Agencies*. Washington, D.C.: National Institute of Justice Research in Brief. January, 1998

ESRI. *Challenges for GIS in Emergency Preparedness and Response*. Redlands, CA: ESRI. May 2000

ESRI. *Geographic Information Systems: A Powerful New Tool for Fire and Emergency Services*. Redlands, CA: ESRI. May 2000

Federal Emergency Management Agency. *National Mutual Aid & Resource Management Initiative; Glossary of Terms and Definitions*. Washington, D.C.: FEMA. December, 2003. [www.fema.gov/pdf/preparedness/glossaryterms.pdf](http://www.fema.gov/pdf/preparedness/glossaryterms.pdf)

Federal Emergency Management Agency. *Support To The Chemical Stockpile Emergency Preparedness Exercise Program*. US Government Procurements. Commerce Business Daily. March 21, 2000

Ferrell, Keith. *XML Consortium Announces Emergency-Response Specs*. TechWeb News. August 12, 2003, [www.techweb.com/wire/story/TWB20030812S0007](http://www.techweb.com/wire/story/TWB20030812S0007)

Ferrolì, William. *Proper Planning Prevents Poor Performance*. Masters Thesis: Rushmore University. November 2002

Gerald, Jeff. ACTD, *Homeland Security; Advanced Concept Technology Demonstration*. Presentation. September 23, 2003  
[www.homelandsecurityactd.org/downloads/HLSC2Brief.pdf](http://www.homelandsecurityactd.org/downloads/HLSC2Brief.pdf)

Hämäläinen, Jorma, Risto Ojanperä and Ari Rahkonen. *Demonstration of Secure ITCM Solution*. Presentation. Information Technology and Crisis Management. September 14, 2003, [www.itcm.org/ppt2/CREATE\\_IBM\\_Secgo\\_14-9-2003\\_v10\\_2.ppt](http://www.itcm.org/ppt2/CREATE_IBM_Secgo_14-9-2003_v10_2.ppt)

Homeland Security Intel Watch *An Emerging Standard for Emergency Interoperability*. Homeland Security Intel Watch, Volume 2, No.1. E.J. Krause & Associates, Inc. January 2004, <http://www.homelandsecurityintelwatch.net/200401/storyinterop.html>

Intergraph Corporation. *Toronto Fire Services Realizes Immediate Benefit After Implementing Intergraph Public Safety's CAD-to-CAD Interoperability Solution*. Press Release. Intergraph Corporation, March 16, 2004

Kennedy, Thomas. *Linking Public Safety to Technology Solutions*. Presentation. Public Safety Technology Center.

Kenyon, Henry S. *Regional Effort Forges Emergency Coordination System*. SIGNAL Magazine. February 2004

McKenna, Ed. *Emergency Management Innovations Aid Government Agencies*. Washington Technology, Post-Newsweek Media. July 5, 1999

MSCMC. *SARS & TOPOFF 2, The Practice, Fear, and Effectiveness of Quarantine*. Presentation. NHSPC. May 2003

Myers, Tom and Bob Welty. *San Diego California, New Technologies To A More Secure Nation*. Presentation. February 2004

National Emergency Management Association Readiness Committee. *Defining the roles and scope of the Information and Warning Technology Subcommittee of the NEMA Readiness Committee*. Position paper. February 27, 2002

National Institute of Justice. *Feature Comparison Analysis Report*. Washington D.C.: National Institute of Justice. January 19, 2003

National Institute of Justice. *Inventory of State and Local Law Enforcement Technology Needs to Combat Terrorism*. Research in Brief. Washington, D.C.: National Institute of Justice. January 1999

National Institute of Justice. *NIJ CIMS Feature Comparison Matrix*. Washington, D.C.: National Institute of Justice. October 2002

National Institute of Justice. *Special Report: Crisis Information Management Software (CIMS) Feature Comparison Report*. Washington, D.C.: National Institute of Justice. October 2002

National Research Council, Committee on Computing and Communications Research to Enable Better Use of Information Technology in Government, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications. *Summary of a Workshop on Information Technology Research for Crisis Management*. Washington, D.C.: National Academy Press. 1999

National Task Force on Interoperability. *Why Can't We Talk? Working Together To Bridge the Communications Gap to Save Lives*. National Institute of Justice. February 2003.

NLECTC-SE. *Critical Incident Response Tool Set Being Tested by South Carolina Emergency Personnel*. NLECTC-SE. February 20, 2003

Office of Science and Technology. *Communications, Information, and Training Technology*. Washington, D.C.: National Institute of Justice. October 2002

RMR & Associates. *Thousands of Assets, Limited Resources: Port Authority of New York and New Jersey Selects Digital Sandbox Site Profiler to Anticipate Threats, Optimize Response*. Press Release. January 15, 2003

The Sphere Project. *Humanitarian Charter and Minimum Standards in Emergency Response*. Oxford, UK: The Sphere Project and Oxfam Publishing. 2004

AP Newswire. *State Receives New Emergency Communications Systems*. AP Newswire. July 3, 2002

Thot-Thompson, Janet. *Multi-sector Crisis Management Consortium*. Presentation. NCSA-ACCESS. MSCMC

United States Fire Administration. *Responding to Incidents of National Consequence. Recommendations for America's Fire and Emergency Services Based on the Events of September 11, 2001 and Other Similar Incidents*. Federal Emergency Management Agency. May 2004

United States Institute of Peace, Crisis Management Initiative. *Towards Interoperability in Crisis Management Conference on Crisis Management and Information Technology*. Helsinki, Finland: Crisis Management Initiative. February 2004

Watson, Dale. Statement to the Subcommittee on Oversight, Investigations, and Emergency Management Hearing on Legislative hearing on H.R. 4210, Preparedness Against Terrorism Act of 2000. <http://www.house.gov/transportation/pbed/hearing/05-04-00/05-04-00memo.html>

Wyke, Allen. *The OASIS Emergency Management Technical Committee: Advancing Incident Management with Open XML Standards*. Interview. EIIP Virtual Forum, <ftp://www.emforum.org/pub/eiip/lc030604.txt>

Zimmerman, Mark. *Disaster Management Initiative*. Presentation. Department of Homeland Security. Created May 30, 2003