System Assessment and Validation for Emergency Responders (SAVER)

Incident Decision Support Software Application Note

August 2010

Homeland Security

Science and Technology

U.S. Department of Homeland Security

SAVER

System Assessment and Validation for Emergency Responders

Approved for public release; distribution is unlimited.

The *Incident Decision Support Software Application Note* was funded under Cooperative Agreement Number EMW-2005-CA-0378 between the Federal Emergency Management Agency, U.S. Department of Homeland Security, and Eastern Kentucky University. Photographs included in this document were provided by Eastern Kentucky University under the cooperative agreement cited previously, unless otherwise noted.

The views and opinions of authors expressed herein do not necessarily reflect those of the United States Government.

Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government.

The information and statements contained herein shall not be used for the purposes of advertising, nor to imply the endorsement or recommendation of the United States Government.

With respect to documentation contained herein, neither the United States Government nor any of its employees make any warranty, expressed or implied, including but not limited to the warranties of merchantability and fitness for a particular purpose. Further, neither the United States Government nor any of its employees assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed; nor do they represent that its use would not infringe privately owned rights.

FOREWORD

The U.S. Department of Homeland Security (DHS) established the System Assessment and Validation for Emergency Responders (SAVER) Program to assist emergency responders making procurement decisions. Located within the Science and Technology (S&T) Directorate of DHS, the SAVER Program conducts objective assessments and validations on commercial equipment and systems and provides those results along with other relevant equipment information to the community in an operationally useful form. SAVER provides information on equipment that falls within the categories listed in the DHS Authorized Equipment List (AEL). The SAVER Program mission includes:

- Conducting impartial, practitioner-relevant, operationally oriented assessments and validations of emergency responder equipment.
- Providing information that enables decision-makers and responders to better select, procure, use, and maintain emergency responder equipment.

Information provided by the SAVER Program will be shared nationally with the responder community, providing a life- and cost-saving asset to DHS, as well as to federal, state, and local responders.

The SAVER Program is supported by a network of Technical Agents who perform assessment and validation activities. Further, SAVER focuses primarily on two main questions for the emergency responder community: "What equipment is available?" and "How does it perform?"

As a SAVER Technical Agent, the Eastern Kentucky University (EKU) Justice and Safety Center (JSC) has been tasked to provide expertise and analysis on key subject areas, including communications and incident decision support software with a focus on the needs of responders from small and rural communities. In support of this tasking, the EKU JSC developed the *Incident Decision Support Software Application Note* to provide emergency responders with information about the components, functionality, and use of software systems that support the management of incidents and multiagency coordination. Incident decision support software falls under the following AEL equipment category: 04AP-05-CDSS, Software, Incident Command System (ICS).

Visit the SAVER section of the Responder Knowledge Base (RKB) Web site at https://www.rkb.us/saver for more information on the SAVER Program or to view additional reports on incident decision support software or other technologies.

POINTS OF CONTACT

SAVER Program
Science and Technology Directorate
U.S. Department of Homeland Security
TSD Stop 0215
245 Murray Lane
Washington, DC 20528-0215

E-mail: saver@dhs.gov
Web site: https://www.rkb.us/saver

Justice and Safety Center
Eastern Kentucky University
50 Stratton Building
521 Lancaster Avenue
Richmond, KY 40475

E-mail: saver@eku.edu

TABLE OF CONTENTS

LIST OF FIGURES

1. INTRODUCTION AND SOFTWARE OVERVIEW

According to the National Incident Management System (NIMS), "[e]ffective emergency management and incident response activities rely on flexible communications and information systems that provide a common operating picture to emergency management/response personnel and their affiliated organizations" (U.S. Department of Homeland Security [DHS], 2008). To help them address these needs at the scene of an incident or within a supporting operations center, emergency response agencies are increasingly turning to software solutions.

There is a wide range of software products currently available for purchase that offer both common and unique features aimed at improving the awareness of key decision makers. The purpose of this *Incident Decision Support Software Application Note* is to provide emergency responders with information about the features, configurations, and use of incident decision support software to assist them in selecting, integrating, and leveraging these tools as part of preparedness, command, and coordination activities.

Unless otherwise cited, the authors collected information for this application note during the market survey of incident decision support software, the first phase in the System Assessment and Validation for Emergency Responders (SAVER) Program process, as well as through Internet research and phone interviews with practitioners.

1.1 Software Overview

Incident decision support software provides Incident Commanders (ICs), emergency managers, and responders with tools to help them manage small- and large-scale incidents and events, coordinate with agencies and responders from other jurisdictions, and communicate critical information. Software supports these outcomes by reducing response times, increasing operational efficiency, and improving the overall management of resources through improved situational awareness.

Some products perform single functions such as resource management, while others are more comprehensive allowing users to employ one computer application to help them perform multiple functions. Emergency management and response agencies in small and rural communities may not have the resources available to purchase multiple software products, or the capability to integrate and manage those products simultaneously during an incident. As a result, these and other types of emergency response agencies may prefer to use comprehensive software applications in their Emergency Operations Centers (EOCs) to conduct multiagency coordination, make resource allocation decisions, and collect and analyze information from many different sources. These sources may range from responders at the scene of an incident to other impacted areas, neighboring jurisdictions, and other operations centers at higher levels of government. See Figure 1-1 for images of active EOCs, which may be ideal work environments for using incident decision support software.

As a tool for supporting multiagency coordination, incident decision support software products are applicable to emergency management, fire service, emergency medical service, law enforcement, and other emergency response agencies that serve a role in the management of incidents. Software packages may be configured to support multiagency coordination in virtual or mobile environments, or at a fixed facility. Most of the software suites available on the market are Web-based tools.

Figure 1-1. EOC Environments *(photos provided courtesy of FEMA)*

Incident decision support software products range in price from a few hundred dollars to more than $50,000. Depending upon the software platform, manufacturers of the software may require monthly maintenance charges or fees for server access or system use. Most manufacturers offer a 1-year warranty with the purchase of their software; however, the base price for many products may not include training and technical support. Also, many software products come with integrated help tools and customer support, which may be provided via e-mail, telephone, and live-chat, for example.

The following sections provide a brief summary of common software features, configurations, information sharing, and security characteristics. Note that these sections do not aim to provide an all inclusive list of purchasing considerations or software requirements; response agencies may have special needs that are not addressed in the following sections.

1.2 Common Features

Commonly-used software applications offer an array of analytical tools to enhance the decision making of emergency responders as it relates to command and control; implementation of plans and procedures; and the allocation of critical resources and tasking for both personnel and equipment. It also provides a means of reporting and maintaining records management and document control for archival purposes. The following incident decision support capabilities are offered in various combinations by manufacturers:

- **Alert and Warning Notification** – This feature allows users to receive and disseminate various types of alerts and warnings. Users may receive and monitor alerts and notifications from different sources to include the National Oceanic and Atmospheric Administration (NOAA) and the U.S. Geological Survey (USGS). As an example, this feature allows for the processing of weather warnings, watches, and forecasts directly to targeted personnel, such as emergency managers, who can then assess the threat and activate an emergency alert to a broader group of affected personnel. The proliferation of Internet Protocol (IP)-enabled software and other devices that leverage the Common

Alerting Protocol (CAP) has made the dissemination of alerts and warnings nearly automatic and in real-time.

- **Geospatial Information (Maps, Imagery, Geographic Information System [GIS] Tracking)** – This function provides visual information about the location of an incident and resources. Many software applications contain mapping programs that display multilayered imagery. They may also provide the real-time geospatial tracking of resources and the capability to integrate and display blueprints and floor plans for buildings. Typically, these applications allow users to capture, store, analyze, manage, and present data that is linked to location. Commonly-used GIS applications include Environmental Systems Research Institute (ESRI) ArcView™ and other ESRI products, Google Earth™, and Microsoft Bing™ maps. Figure 1-2 shows an example software application that provides a mapping capability to allow users to identify, for example, ingress and egress routes and the location of assets and infrastructure.

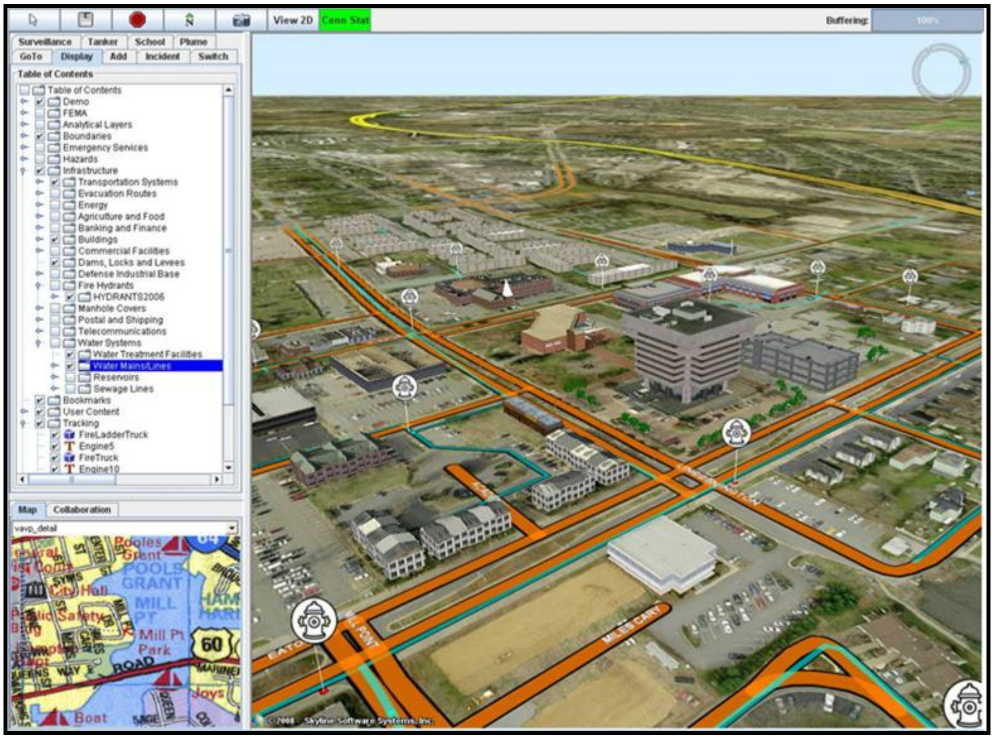

Figure 1-2. Example Mapping Application

- **Incident Notification and Messaging** – This feature supports incident notification and situation reporting. This may be accomplished through interfaces with other systems or integration with public and private databases to provide real-time situational awareness. An example of this capability includes receiving, completing, and processing Incident Command System (ICS) forms, such as the ICS 209 (Incident Status Summary). Many comprehensive software packages include a Records Management System (RMS) to assist users in archiving incident reports. They may also provide automatic reporting capabilities such as Enhanced 9-1-1 (E911), which automatically associates a physical address with the calling party's telephone number to assist the agency in identifying the appropriate response assets.

- **Resource Management** – Resource management provides the capability to inventory and quickly identify Federal Emergency Management Agency (FEMA) typed and other resources, order and acquire resources, and track and report on the status of resources. Resource management applications may provide or be linked to Computer-Aided Dispatch (CAD) systems used at 9-1-1/dispatch centers or other resource ordering systems. They may also be shared with or connected to other agency's or jurisdiction's information management systems to support mutual aid operations. During the recovery phase, resource management features allow users to recover/demobilize assets and support reimbursement.
- **Modeling and Simulation (Plume, Weather, Forecasting)** – This feature provides emergency responders with information on natural and infrastructure risks, forecasts incident consequences, and analyzes the impact of hazards based on demographic data and human needs. Modeling and simulation capabilities may assist emergency responders in assigning rescue personnel and equipment; organizing medical support; and monitoring weather conditions, environmental problems (toxic plumes, etc.), and evacuation routes. During the preparedness phase, this feature may be used to support simulated training to improve operational readiness and response to catastrophic events. Figure 1-3 provides an example of a weather-related modeling and forecasting application that would be useful for supporting operational decisions and exercises.

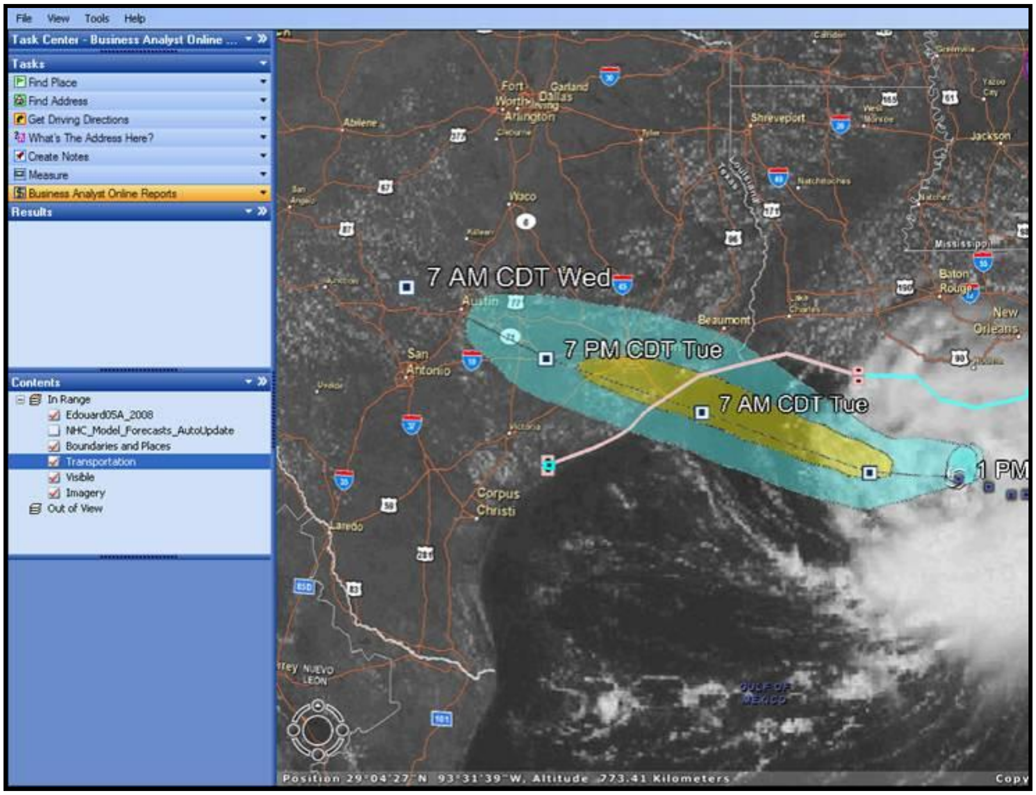

Figure 1-3. Modeling and Forecasting Application

- **Surveillance and Analysis (Damage Information, Responder Authentication, Intelligence)** – Capabilities in this category may include video analytics, streaming video and audio coding, and data and processing/storage capabilities, which are integrated into a single interface that can be operated by multiple users. Examples of surveillance and analysis software include applications that support the sharing of camera feeds from remote locations back to the operations center or command post for displaying and storing information. The use of cameras and other sensors may be used in support of physical security, access control, and surveillance. Site security applications may be integrated with software that provides a database and runs checks of identification cards for personnel authentication and accountability purposes. Also, software in this category may support multi-source collection and the production and dissemination of intelligence to incident response organizations so they can monitor threats, detect and prevent attacks, and alert authorities.

There are also software products that provide middleware such as data mining and gateways for supporting communications and networks that may be invisible to the end user, but fulfill important backbone and infrastructure requirements.

Not all communities may need all of these features built into a comprehensive software suite. Small and rural communities may not have the resources available to purchase the software or the staff needed to effectively operate and benefit from the applications. Some features may be best used at a command post location (e.g., site security applications), while others may be better used in an EOC environment. For example, command post personnel may be focused on tactics and need a basic software application to support the development of the Incident Action Plan (IAP). In contrast, the EOC may need a robust package of capabilities to assist in the coordination among all emergency support functions. See Section 2 for additional purchasing and operational considerations.

1.3 Configurations and Information Sharing

Software packages may be configured as a virtual, Web-based solution, part of a mobile setup to support the emergency response, or utilized at a fixed facility. Software products may be utilized in a number of ways, including over the public Internet, on a private intranet, or via a Local Area Network (LAN) as a means to coordinate and deliver emergency response information instantly or within an appropriate period of time. Many software products have system requirements for hardware, which encompass Web servers and/or database servers, as well as architectures for managing databases such as Structured Query Language (SQL) and other applications. Microsoft® SQL Server® is a commonly-used relational database management system for products maintained at the local user level.

One of the key indicators in selecting the appropriate software is what the agency requires the software to do in capturing and disseminating information. Many of the software products provide real-time data collection and dissemination, which helps to increase situational awareness and reporting capabilities. Generally, software products can be configured to allow responders to exchange information in multiple formats such as documents, Short Message Service (SMS)/text messages, emails, data files, videos, audio, and images among agencies in a timely and effective manner.

Many software applications can display and export images in ordinary file types, such as Joint Photographic Experts Group (JPEG), Graphics Interchange Format (GIF), and Bitmap (BMP) formats. Data is exported using common formats and file types including Comma-Separated Values (CSV), Text (TXT), and Extensible Markup Language (XML) files. Response agencies may want to ensure that the exported file types are compatible with other agency computer programs. Most applications provide a means to save files to external media such as optical discs (e.g., Compact Discs [CDs], Digital Video Discs [DVDs]), Universal Serial Bus (USB) flash drives, or stored on the hard drive itself.

Applications that rely on one or more servers allow users to post information for others to view or retrieve for their awareness; these servers may also be used as hubs for sharing data across many users of a proprietary system. Data interoperability with disparate commercial and government products and different types of equipment (e.g., cellular phones, Personal Digital Assistants [PDAs], smart phones) is often achieved through the use of commonly-accepted data messaging standards such as the Emergency Data Exchange Language (EDXL) suite of standards.

The EDXL CAP standard, for example, is gaining popularity as a means of exchanging all-hazard alerts and warnings over the Internet, including Emergency Alert System (EAS) messages. The CAP standard has afforded users of incident decision support software to increase the range of platforms that can receive alert and warning messages, as well as the integration of other forms of multimedia. Moving Picture Experts Group (MPEG) Audio Layer 3 (MP3) files with audio messages can be transferred through CAP. Weather alerts and watches can also be more compatible for SMS/text messaging. More and more subscription services are being offered in a variety of counties across the country. Subscribers who register for weather alerts can also receive National Weather Service (NWS) bulletins because CAP provides a conduit for messages to be entered and packaged for text messages. Many incident decision support software products integrate CAP, which allows users to use the software as a means of disseminating all types of alerts.

Additional EDXL standards allows for messaging among users of different software systems for other purposes, such as to request resources and to share information about hospital capacity and bed space. The National Information Exchange Model (NIEM) supports the exchange of EDXL-based and other types of standards by providing common semantics and packets for exchanging information across agencies for specific operational purposes (e.g., America’s Missing: Broadcast Emergency Response [AMBER] Alerts). See Section 1.5 for additional information about standards.

1.4 Information Security

According to NIMS, “[p]rocedures and protocols must be established to ensure information security” (DHS, 2008). Response agencies should determine if the security features offered with the incident decision support software supports their agency’s information security policies and protocols.

Most commercial software products provide a login feature and individual accounts set up by an authorized person that requires usernames and passwords for accessing information. This layer of security ensures that only authorized individuals are allowed to access the software and insert and retrieve data. Software products that also provide a log of activity help agencies with identifying and investigating potential security issues. Web-based software products have security risks commonly associated with other Internet products. Users should ask manufacturers about network security before purchasing an account to ensure it meets their agency's requirements.

Agencies must also ensure that software applications come with mechanisms to back up and retrieve incident data, which may be an additional cost for agencies. Certain products come with automatic database back up features. Agencies should also consider archiving databases and files regularly on a separate computer system for records management and operational redundancy purposes.

1.5 Standards and Resources

The need for data interoperability, a common operating picture, and information security has led to the development of standards; the following list provides a few key standards and resources that response agencies may reference when selecting software solutions:

- American National Standards Institute (ANSI) InterNational Committee for Information Technology Standards (INCITS) 415: Homeland Security Mapping Standard – Point Symbology for Emergency Management
- Institute of Electrical and Electronics Engineers (IEEE) 1512: Standard for Common Incident Management Message Sets for Use by Emergency Management Centers
- National Fire Protection Association (NFPA) standards, including NFPA 1221 (Standard for Installation, Maintenance, and Use of Emergency Services Communications Systems)
- Organization for the Advancement of Structured Information Standards (OASIS) Emergency Data eXchange Language (EDXL) standards
- U.S. Department of Homeland Security Geospatial Data Model (GDM) and other products and standards endorsed by the Federal Geographic Data Committee (FGDC)
- U.S. Department of Homeland Security SAFECOM Program
- U.S. Department of Homeland Security and U.S. Department of Justice National Information Exchange Model (NIEM)

Many standards organizations such as OASIS continue to develop data standards based on the needs of emergency responders. See Appendix A for a list of Web sites that provide information about newly-developed standards.

There are two resources that practitioners can reference when considering a new purchase or system configuration, developing Requests for Proposals (RFPs) for new products, or conducting self assessments of existing information management systems. In 2002, the National Institute for Justice (NIJ) sponsored the Crisis Information Management Software (CIMS) Test Bed Project to assist response agencies in comparing and contrasting commercially available software (NIJ, 2002). Although the products featured in the project report have changed, the overview and criteria used in the assessment are still valuable.

More recently, FEMA is sponsoring the NIMS Supporting Technology Evaluation Program (NIMS STEP), which provides an objective evaluation of incident management software against NIMS concepts and principals (e.g., accountability, resource management, unified command) (FEMA, 2009). Summaries of NIMS STEP reports are made available on the Responder Knowledge Base (RKB) Web site at https://www.rkb.us (keyword search: NIMS STEP).

1.6 Limitations

There are limitations with incident decision support software applications, which could impact response agencies. The following provides a sample list of software limitations.

- **Managing New Releases** – Software technology tends to evolve very quickly as compared to hardware; new versions of software with new capabilities are generally released more often than their hardware counterparts. An additional burden for agencies that regularly train on and use incident management software is the need to manage new releases and updates from infrastructure configuration, training, and operational perspectives.
- **Proprietary Software** – Many commercial products are developed using proprietary applications and software rather than based on open standards for supporting interoperability and the exchange of data with other systems.
- **Security and Redundancy** – Inherent with any information management system is the security of incident data, which presents new risks and costs to response agencies. These risks include the accidental or criminal release of sensitive information, and the loss of data due to a system failure or loss of power.
- **Reliance on the Internet** – Like communications systems, the Internet is susceptible to failures during disasters due to power failures and/or severed wire connections. Software applications managed by a third-party vendor or locally through a network could become inaccessible.
- **Service Fees and Licenses** – Some manufacturers charge monthly service fees to response agencies for accessing and using applications, especially those that are managed in a virtual environment by the manufacturer. Also, it is not uncommon for manufacturers to charge agencies for individual user licenses and accounts.
- **Not a “Silver Bullet”** – Software applications are not a solution for reducing all of the complexities and challenges associated with the management of incidents, or a replacement for planning, training, and exercises, as well as other preparedness activities required for effective response and recovery. Likewise, training on the use of software should be part of an organization’s training program.

2. APPLICATIONS

Although incident decision support software may be used at the incident scene to support tactical-level decisions, the comprehensive applications are more likely to be employed within the EOC environment in support of multiagency coordination functions and decisions regarding resource allocation. At all levels of command and coordination, software can be used to manage all phases of an incident from the preparedness phase to the response and recovery phases. The following sections provide examples for how incident decision support software may best apply to the incident command, multiagency coordination, and emergency preparedness functions.

2.1 Incident Command Considerations

During the initial stages of an incident, responders and the IC or the Unified Command (UC) are likely coordinating directly with the local dispatch center or department operations center with status reports and resource requests. At this phase in which life safety is the priority, orders are typically provided by the IC/UC verbally and responders use Land Mobile Radios (LMRs) to communicate and share information. The use of incident decision support software becomes more relevant and useful as the incident expands and resources arrive on scene that require management.

Software may be pre-installed on a mobile command system or mobile command vehicle for use during the initial stages of an incident. Software features that may be the most useful are those that provide automated notifications, maps of the incident scene, and a way to compile a list of resources. These features may be provided separately or built into automated ICS forms.

Software applications may support the ICS sections in various ways. Tactical and discipline-specific applications would be helpful in support of the operations function. For example, medical personnel may benefit in using software that provides a list of local medical facilities, hospital types, and available bed space. A resource management application may make the work of the resources unit and the logistics section more efficient. Records management applications might assist the documentation unit and the finance/administration section with their responsibilities.

If the incident response is prolonged, the command staff may need to plan for future operational periods. In these circumstances, incident decision support software could be used to support the various steps in the development of the IAP. See Figure 2-1 for examples for how software could support the development of the IAP.

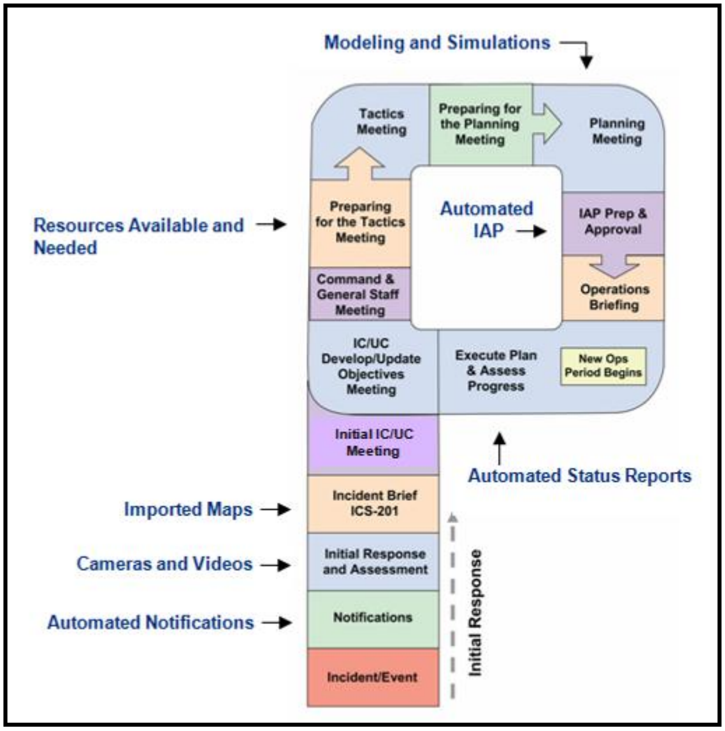

Figure 2-1. Software Support for Planning (Examples)

2.2 Multiagency Coordination

As the incident escalates and the need is identified for significant resources, EOCs and other multiagency coordination system components are activated. EOCs help form a common operating picture of the incident, relieve on-scene command of the burden of external coordination, and secure additional resources. EOC personnel play a critical role in acquiring, allocating and tracking resources, managing and distributing information, and setting response priorities among many incident sites. As such, incident decision support software may be used as a tool in support of these complex activities and requirements.

Information from all sources and impact sites can be consolidated using software for a global view of the disaster allowing analysis and appropriate and timely decision-making that provides effective support to department operations centers and ICs in the field. Specifically, software may be used to support the primary functions that take place at the EOC, including:

- **Communications Facilitation** – Establishing interoperable communications among all partners in the multiagency coordination system and others, as necessary for the response.
- **Coordination** – Coordinating the information flow and resources for complex incidents or multiple incidents occurring simultaneously.
- **Information Collection and Evaluation** – Collecting, analyzing, and interpreting information from various sources.
- **Priority Setting** – Making decisions based on agreed-upon policies and procedures.
- **Resource Coordination** – Identifying and acquiring needed resources and allocating existing or known resources.

Software that supports information sharing becomes critical at the local, regional, and state coordination levels. For example, software may be used to support the real-time sharing of information between the IC and the local EOC. Likewise, information from the local EOC may be accessed by the state EOC for their awareness and in support of resource requests that they may need to help coordinate. The use of Web-based software applications may be the most appropriate tool for response to these complex incidents. See Figure 2-2 for an illustration of possible information sharing pathways that may need to be supported through the use of incident decision support software.

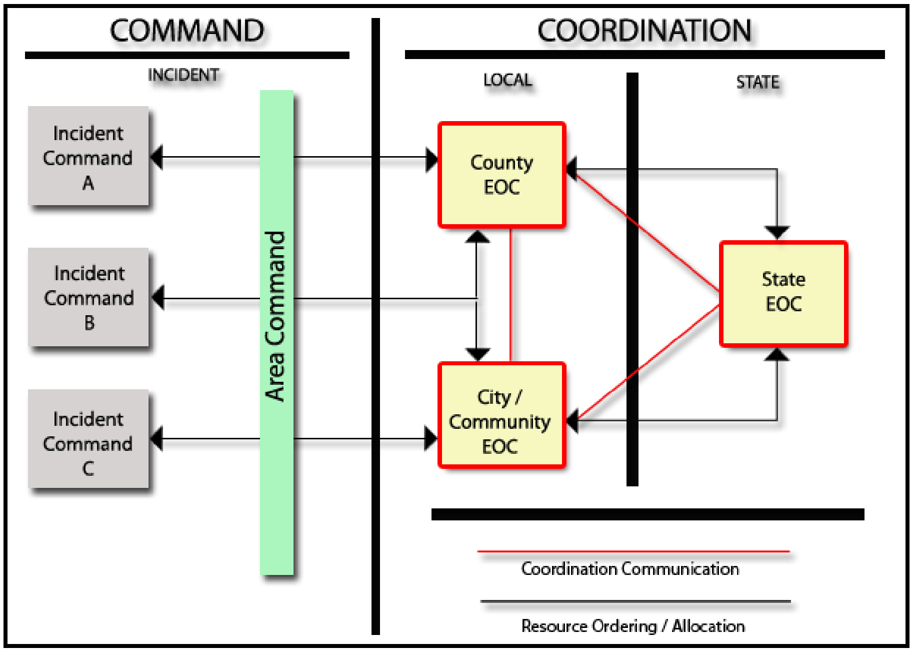

Figure 2-2. Software Support for Coordination and Information Sharing (Examples)

Incident decision support software may also be used as a flexible tool for use in planning for and managing events at any level that require coordination across many public safety disciplines. These events could range from parades, fairs, festivals, and concerts at the local community level to sporting events that draw a significant number of people at the regional level to National Special Security Events (NSSE). Software may be used to quickly identify the location of security personnel and the public, as well as other staged responders that may be needed in case of an incident. It may also be integrated with event location surveillance cameras to provide the management team at command posts or operations centers with a common operating picture.

2.3 Preparedness

Another common use of incident decision support software is as a preparedness tool for emergency response planning, the identification of hazards and risks, and conducting exercises, among other activities. Many software systems come installed with the following examples of preparedness aids:

- Planning templates and checklists.
- "One stop" repositories for policies, plans, procedures, and mutual aid agreements.
- Database for populating contact information for key personnel and other stakeholders.
- Resource inventories and links to registries for persons with special needs.
- Models for identifying risks based on hazard types and occurrences, critical infrastructures and key assets, and population centers.
- Simulations that may be used in support of exercises, including features that allow agencies to capture lessons learned and develop after action reports.

3. CONCLUSION

In summary, incident decision support software products, if used appropriately, help emergency responders in managing incidents of any scale or complexity by providing access to critical incident-related information. The focus of this report is on the use of comprehensive software applications that provide situational reports, geospatial/visual information, and the status of resources within a single portal/user interface. Advanced software packages may include many more features, some of which are described in Section 1, as well as real-time information sharing and alert and warning capabilities.

Please note that software technology tends to evolve very quickly as compared to hardware; new versions of software with new capabilities are generally released more often than their hardware counterparts. Agencies need to manage these changes and account for the other limitations identified in Section 1.6 when purchasing and using incident decision support software.

The *Crisis Information Management Software (CIMS) – Feature Comparison Report* notes that agencies should consider the following regarding incident decision support software:

- There is no best product.
- There is no perfect fit.
- The best product for your agency should be based on:
    - Budgets
    - System environment
    - Scale of operation
    - Sophistication of operation
    - Discipline to implement
    - Political considerations (NIJ, 2002).

Software used in a mobile command post may not meet the multiagency coordination needs of a local or state EOC. Likewise, comprehensive software used in EOCs may be too onerous and complex for a command post. Agencies from rural communities with few computers and little infrastructure may need client-based software. Metropolitan agencies may need advanced networking and Web-connected applications to achieve their coordination needs.

Regardless of software configuration or complexity, agencies should consider purchasing products that conform to data exchange standards to achieve a minimum level of data interoperability and NIMS requirements.

APPENDIX A – REFERENCES

American National Standards Institute (ANSI): http://www.ansi.org.

Federal Emergency Management Agency, U.S. Department of Homeland Security (2009, December). *National Incident Management System Supporting Technology Evaluation Program (NIMS STEP) Guide*. Retrieved from: https://www.nimsstep.org.

Federal Geographic Data Committee (FGDC): http://www.fgdc.gov/.

Institute of Electrical and Electronics Engineers (IEEE): http://www.ieee.org/portal/site.

National Fire Protection Association (NFPA): http://www.nfpa.org.

National Institute of Justice, Office of Justice Programs, U.S. Department of Justice (2002, October). *Crisis Information Management Software (CIMS) – Feature Comparison Report.* Retrieved from: http://www.ncjrs.gov/pdffiles1/nij/197065.pdf.

Organization for the Advancement of Structured Information Standards (OASIS): http://www.oasis-open.org.

Responder Knowledge Base (RKB): https://www.rkb.us.

U.S. Department of Homeland Security (2008, December). *National Incident Management System*. Retrieved from: http://www.fema.gov/emergency/nims/.

U.S. Department of Homeland Security and U.S. Department of Justice National Information Exchange Model (NIEM): http://www.niem.gov.

APPENDIX B – ACRONYMS/ABBREVIATIONS

The following acronyms/abbreviations are commonly used in this document.

Acronym/ Abbreviation	Definition
CAP	Common Alerting Protocol
DHS	U.S. Department of Homeland Security
EDXL	Emergency Data Exchange Language
EKU	Eastern Kentucky University
EOC	Emergency Operations Center
FEMA	Federal Emergency Management Agency
GUI	Graphical User Interface
IAP	Incident Action Plan
IC	Incident Commander
ICS	Incident Command System
NFPA	National Fire Protection Association
NIEM	National Information Exchange Model
NIJ	National Institute of Justice
NIMS	National Incident Management System
OASIS	Organization for the Advancement of Structured Information Standards
RKB	Responder Knowledge Base
SAVER	System Assessment and Validation for Emergency Responders
S&T	Science and Technology Directorate, U.S. Department of Homeland Security
UC	Unified Command
U.S.	United States of America