Unified Incident Command and Decision Support (UICDS)

A Department of Homeland Security Initiative for Information Sharing Among Commercial, Government, Academic, and Volunteer Technology Providers to Support the National Incident Management System

UICDS is All About Content: Turning Data into Actionable Knowledge

I. Overview

In an emergency operation today – whether responding to an actual event or to indications and warnings coming from an intelligence agency – each person, team, and organization knows about their own information. Police know police, fire knows fire, counter-terrorism knows counter-terrorism. But, these response forces operate virtually in isolated information silos … until each shares their information *as they are able and enabled.* This results in gaps, overlaps, and inconsistencies in who knows what, when, which yields isolated information and clouded decision making.

Extend this problem from a single town or city to a large-scale disaster with many cities, a couple of states, a dozen federal agencies, numerous volunteer organizations, and hundreds of private sector, critical infrastructure owner/operators and you begin to see the scope of the problem and the scale of the needed solution for information sharing in incident management.

II. Not Just a Pretty Picture

The Broad Agency Announcement that launched Unified Incident Command and Decision Support (UICDS) set the following set of objectives: "The full capabilities of information management technologies should be brought to bear on behalf of the first responder community in the form of a system that allows first responders to manage the flow of data, voice, and video information in addition to other forms of information." More specifically, UICDS should enable "the capabilities that allow emergency responders to capture important incident-related information, analyze captured information, more effectively disseminate mission-critical information to emergency responders, present decision guidance options for the emergency response community, efficiently coordinate efforts of emergency responders, and store incident-related information for analysis." In short, the goal of UICDS is to share information across domains, across roles, across functions, across echelons, across hazards, and a cross applications. This is more than a common operating picture created by bringing disparate data into a single new application that everyone must use. It is more than situational awareness providing a new summary application everyone must use. It is true information sharing among applications that enable each individual application – selected for its intrinsic value by an end-user organization – to acquire common data and compose that data into a visualization that is appropriate for the end-user. The application then can further process that data and resubmit it for sharing with the originating – and other interested – applications. UICDS is not one size fits all; one application cannot meet all needs. UICDS builds many-to-many relationships among applications to meet the unique needs of very diverse end-user communities.

III. It's All About the Right Content

Content is what is critical to the five million – and perhaps more than 10 million –emergency management personnel across the United States at all levels of the federal, state, local, and tribal governments and the private sector that will have access to UICDS information sharing through the applications that they use every day. These millions of UICDS users come from thousands of organizations that are joined in 24x7x365 net of information from which their applications select content that is relevant for each individual and the teams and organizations within which they operate. UICDS is all about delivering the "right content" at the right time to manage an incident.

Unified Incident Command and Decision Support is being developed under contract to the Department of Homeland Security (DHS), Directorate of Science and Technology (S&T) by Science Applications International Corporation, McLean, VA 22102 USA. James W. Morentz, Ph.D. is a Homeland Security Technology consultant (phone: 301-467-4242; email: morentzj@saic.com). Christopher Doyle is director of the Infrastructure and Geophysical Division of the DHS S&T Directorate. Lawrence Skelly is deputy director of the Infrastructure and Geophysical Division of DHS S&T. Nabil Adam, Ph.D. is technical lead for the UICDS project and fellow and senior program manager at DHS S&T. Tomi Finkle provides program support for the DHS S&T UICDS project. The UICDS team includes Project Manager Chip Mahoney, Roger Wuerfel, William Summers, Daniel Huang, Daphne Hurrell, and Roberta Blake Marietta. Subcontractors to SAIC are Image Matters, KZO Innovations, and Constellation Software Engineering. Earlier versions of this paper were presented at the IEEE Homeland Security Technology Conferences in May 2008 and 2009 and appear in conference proceedings.

Each UICDS end-user is interconnected through open-standard interfaces among commercially available applications and devices that are familiar to them – their computer software, existing phones, personal digital assistants (PDAs), mobile data terminals, radios, and whatever digital device may emerge in the future. These end-user applications and devices have the primary function of exchanging normal, everyday information but, when UICDS-enabled, form a network of knowledge about every incident.

What UICDS provides on these existing communication devices is shared information by linking together relevant applications with data that pertains to an incident. UICDS understands the difference between a house fire and an industrial fire when entered in a dispatch system being monitored. Because the industrial fire poses a risk of industrial chemical hazards, UICDS Information Sharing Agreements are composed to notify interested applications of the industrial fire while ignoring the house fire. Other applications subscribe to the industrial fire incident and benefit from how UICDS distills thousands of possible pieces of information into the essential elements of information needed for decision-making by specific people in specific roles at specific times in an emergency.

Selecting the "right content" from among thousands of systems is accomplished by UICDS Agreement and Profile Services. Agreements create relationships among UICDS organizations and Profiles create relationships among UICDS applications allowing each user to acquire, analyze, and display mission-critical information specifically needed for the decisions the end-user will make.

The "right content" is that fraction of all the data created by an application or a set of applications that helps an end-user make the right decision about saving lives, property, and the environment. It will always be difficult to decide exactly what that fraction of data is in any given incident. But, with UICDS, there is a very good chance that the composite of data about the incident can be composed into the "right content" for three reasons.

First, UICDS consumes data from applications that know their end-users well. And end-users have selected the applications that best represent their interests and needs because those applications best process and represent the necessary, detailed data needed by the agency or individual to get the job done. The quality of the application as it meets the needs of the end-user is the first reason that data residing in UICDS can become the right content.

Second, UICDS transports a carefully selected fraction of the detailed data that an application uses to manage its full mission. It is this fraction that is valuable to manage the overall, multi-agency coordination. This fraction of data is based on the National Incident Management System plus input from stakeholder representatives plus several data standards that are the result of thorough consultation among knowledgeable people. The NIMS doctrine, the standards of expert organizations, and the input of practitioners all combine to make the data in UICDS of inherent value in describing an incident.

Third, the composition of the right content takes place in an application that the end-user knows. There is no new user interface, no new training, no new applications imposed by UICDS. Rather, UICDS data is visualized in the form and substance the end-user selected to manage their own mission. Familiarity breeds understanding and results in the "right content" for the needed decision.

IV. The UICDS Tree of Knowledge

UICDS builds a knowledge base about any incident by compiling a series of UICDS Work Products composed of data provided by applications interfaced to UICDS through the application's UICDS Adapter. The adapter authenticates the applications to connect to UICDS Web Services and translates into a standard format the detailed data of the application into the fractional data to be shared with UICDS. Thus, the UICDS Work Product is the basic unit of data exchange among applications. Each application provides data when it has something to contribute to the incident knowledgebase and consumes a work product when it wants its end-user to know about the incident. The content of a UICDS incident is illustrated in figure 1 and described below.

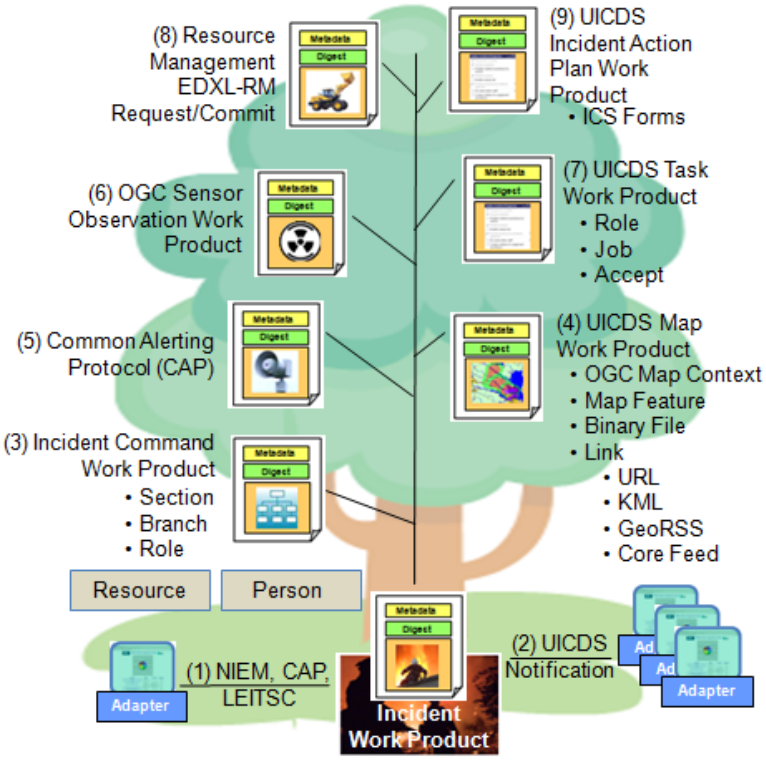

Figure 1. UICDS transports data among the providing and consuming applications that represent the whole range of critical information on the incident who, what, when, where, and how: geospatial, sensors, command structure, personnel, resources, alerts, operating procedure tasks, and action plans.

An incident may be created (1) by any of a number of emergency applications – computer-aided dispatch, sensors, traffic cameras, EOC software, or others. The origin of that incident may be an actual event or an indication or warning of an impending event. Whatever the source, any application that is UICDS-enabled can create an incident when their UICDS Profile gives them incident creation permissions.

UICDS consumes messages indicating that an incident is being tracked by an application in three different standard formats, the Common Alerting Protocol, the National Information Exchange Model incident description, and the primary law enforcement dispatch incident standard from the Law Enforcement Information Technology Standards Committee (LEITSC).

Upon receipt of an incident from an application, UICDS broadcasts (2) a notification of the incident to all connected applications who have subscribed to that type of incident. This broadcast employs the Web Service for Notifications standard. The UICDS implementation of notifications and the UICDS Agreement Service allow each application to assure that its end-users will not receive incident notifications about anything that is irrelevant to their mission. Relevancy can be determined by a number of measures including type and geographic proximity.

UICDS structures all the disparate information being created by a number of applications being used by a number of agencies into its knowledgebase. When an incident is created by an application, an Incident Command System structure is created (3). ICS is the basic unit of organizational response to an emergency as established by the National Incident Management System. As people and resources are dispatched to the scene of the incident, those dispatch and resource management applications update the command structure. No matter whether the allocation of a person or resource came from fire or police or health or the state or a neighboring jurisdiction, UICDS helps to cross all those boundaries to create a consolidated management structure, thus answering the key question: Who is in charge?

Just as important as who, is where? Thus, when an incident is created, UICDS automatically creates a base map of the area in which the incident occurs in the form of an OGC Map Context document (4). This allows any application with geospatial information related to the incident to permit UICDS authorized end-users to view that geospatial information on their own viewing application. In addition, UICDS allows applications involved in the incident to identify and include Map Features in UICDS work product documents as well as Binary Files (photographs or aerial imagery, for example). Finally, the UICDS map also allows feeds, such as RSS, GeoRSS, KML, and URLs to be associated with the incident by an application.

UICDS handling of such feeds is important to avoid information overload. In any area there may be dozens of feeds, each having a number of items. For example, there may be feeds for stream gauges, rain gauges, traffic speed sensors, traffic lights, traffic accidents, criminal acts, 311 service calls, news reports, and dozens of others. Each of these feeds has multiple items – a reading or report at a location. For example, the traffic speed sensor at 4th and Main, 10th and Broadway, 15th and I-66, etc. Thus, the number of items for relevant feeds related to the safety and security could number in the hundreds.

How to make sense of what is important?

UICDS allows applications to make sense of all these feeds. If an incident occurs at 3rd and Main, a Department of Transportation application may automatically, or with user intervention, select the 4th and Main traffic speed sensor to be included with the UICDS incident information. Personnel in other agencies do not have to sort through all the feeds to find the one that helps them make a decision. Rather, information experts and analysts build the UICDS incident knowledge tree so that operations personnel can quickly understand the incident and do their job of protecting their assets and services.

Throughout the course of an emergency, alerts (5) are provided by various applications and become part of the UICDS incident knowledge. UICDS has adopted the Common Alerting Protocol (CAP) as its standard description of an alert. If an application disseminates CAP messages, UICDS can consume them and associate them with an incident, thus building incident knowledge. When an application wants to know what alerts are associated with an incident, it obtains the CAP UICDS Work Product and, because it is in the CAP standard format, can understand the content of the CAP message.

UICDS does not take away the mission of alerting applications. They remain the system of record and their time-critical delivery of vital messages goes unimpeded. The role UICDS plays is to be a consumer of an alert and then to notify UICDS subscribers that an alert has taken place. Thus, agencies and individuals that are not part of the alerting system of record know that alerts have been issued.

UICDS extends incident knowledge by allowing sensors (6) to be included in the available incident information. Using the Open Geospatial Consortium Sensor Observation Service standard format, sensor applications can identify the availability of sensor data related to the incident and publish that availability to the UICDS Sensor Work Product. Thus, UICDS points the end-user application to any subscribing traffic cameras or weather sensor or chemical sensors that the contributing emergency management sensor applications are offering to support the emergency response. In this way, the UICDS incident knowledge expands and is constantly updated with the latest sensor information.

During an emergency, people and organizations are engaged in a wide variety of activities, all of which are part of the necessary knowledge about an incident captured in the UICDS Task Work Product (7). Applications that specialize in Standard Operating Procedures (SOPs) and tracking of the performance of such procedures are the sources of data for the UICDS Task Work Product. As jobs are assigned to individuals performing roles in the response, those applications provide such data to UICDS. UICDS then relates that data about procedures, assignments, roles, and status to the incident and makes each successive update of the work product available to those applications consuming the incident. Those applications, in turn, use the task data to visualize for

their end-users the current status of procedures and tasking for the incident.

Sharing of information about on-going response resources used in carrying out SOPs is accomplished through UICDS Resource Management Work Products (8). UICDS has adopted the primary emergency management resource standard, Emergency Data Exchange Language-Resource Messaging (EDXL-RM). UICDS enables the exchange of all of the EDXL-RM messages that allow applications to request resources, inquire about resources, negotiate their delivery, track their use, and eventually return or replace the resources through the EDXL-DE standard. UICDS develops Resource Management Work Products specifically to enable the request and commitment of resources. The fractional data from the EDXL-RM exchange that UICDS tracks and makes available to other applications is the request/commit of EDXL-RM. Thus, resource management applications remain the systems of record for the resource negotiation while UICDS shares with all applications the need for resources and the satisfaction of that need.

With people, organizations, resources, assignments in place, the final piece of incident knowledge is the record-keeping that leads to planning for the next response period. UICDS maintains the Incident Action Plan Work Product (9) which is a representation of several Incident Command System (ICS) forms that culminate in an Incident Action Plan. The purpose of this service is to support ICS forms that enable an incident to be managed at the incident commander level. This allows information sharing and reporting on the status of the incident, future requirements, and action plans to be undertaken.

All these elements of incident knowledge that are shared through UICDS add up to the UICDS Tree of Knowledge. If you look at these nine information clusters, you will see all the critical information that is now shared around a conference table in an Emergency Operations Center. People, plans, resources, observations, alerts, responsibilities … these are the elements of incident management that are currently in silos and which become a coherent whole through the sharing of individual application data to the composite of all applications serving the end-users making decisions in an emergency.

V. Fractional Data, Standards, UCore Digests, and UICDS Work Products

A basic principle of UICDS is that the jurisdiction/end-user/application owns the Detailed Data to manage a response because the application user owns the response. The role of UICDS is not to manage that agency response. Rather, UICDS is designed to help the overall managers and incident commanders manage the relationship among the managers of agency responses. The principle of contributing to information sharing for multi-agency response is embedded in the doctrine of the National Response Framework and the National Incident Management System upon which UICDS is designed.

To accomplish this, UICDS adopted the concept of "fractional data." Detailed data is needed to manage an agency response. Some "fraction" of that detailed data is needed to manage the relationship among agencies.

Fractional data was defined throughout Phase I of the UICDS development in which numerous end-user outreach activities were held to determine what key data is needed to perform the overall NIMS-based management of an incident. In addition to this end-user input, the UICDS team also examined existing data exchange standards. This was done because standards are the result of many previous end-user interactions to achieve a consensus on some element of information exchange. When a standard existed, there was no need to examine anything more than its appropriateness for inclusion in UICDS.

Among the standards currently incorporated in UICDS as a means to define or exchange this "fraction" of the detail data that is shared through UICDS to manage the relationship among response organizations are:

- National Information Exchange Model (NIEM)
- Common Alerting Protocol (CAP)
- EDXL-Distribution Element
- EDXL-Resource Messaging
- UCore Digest
- Open Geospatial Consortium (OGC) Web Map Context
- OGC Web Mapping Service
- OGC Web Feature Service
- OGC Sensor Observation Service
- KML, GeoRSS, and Atom+GML
- Law Enforcement Information Technology Standards Council (LEITSC)

The careful observer will note that some of these standards overlap, even conflict. Earlier, it was noted that UICDS accepts three different formats for initiating an incident, NIEM, CAP, and LEITSC. This is because some incidents begin with an alert (CAP), some are composed by an application structuring its incident description according to the emergency management standard (NIEM), and other incidents commonly come from the law enforcement community standard for dispatch exchanges (LEITSC).

So, how does UICDS make sense of these "different" standards?

By employing a standard for summarizing data, UICDS automatically creates "Digest Data" based on the Department of Defense originated (but now adopted by dozens of organizations) Universal Core, or UCore, standard that summarizes Who, What, Where, and When of UICDS Work Products. This allows cross-standard understanding of UICDS data.

Thus, a UICDS Work Product consists of (a) the "payload" containing fractional data selected by an application adapter from the applications detail data, (b) the UCore Digest that summarizes the fractional data, and (c) metadata that consists of ULex derived metadata components to capture Identification and property elements required for the UICDS infrastructure and to enable the adapter to process the work product. UICDS Work Products are the atomic unit of UICDS information sharing. A Work Product is a versioned artifact so that applications know they have the most current data and can

use historical work products for analysis if they wish. Work Products may be generated by UICDS services, external data sources, or by UICDS client applications.

Figure 2. Chris McIntosh, then-Deputy Director of Operations for the Virginia Division of Emergency Management highlighted the primary value of UICDS for state and local governments when he said: "Through the commonality and data interoperability which this program [UICDS] is promoting, it allows a million dollar ESRI™ investment or a free copy of Google Earth™ to visualize information. And that's what's truly powerful because you're not pushing business requirements on the locals, you're not making everybody come to our system, or the federal government's not making every state come to their system, you're able to leverage what you have already."

VI. UICDS Deployment Options

UICDS accomplishes all this by distributing a decentralized network of, perhaps, thousands of UICDS core units with capabilities matched to end-user needs. For example, a large city, state, or multijurisdictional region's UICDS installation may be a network of UICDS core servers fully integrated with Computer-Aided Dispatch (CAD), traffic sensors, hospital admissions systems, public works equipment maintenance records, arrest and warrant management systems, weather sensors, and more. Scale down deployment of UICDS to a single computer, lower communication bandwidth, and fewer integrated external systems and UICDS serves any type or size of community – urban or rural, coastal or desert, ski resort or football stadium, multiagency and multijurisdictional. The ability of UICDS's peer-to-peer architecture to scale in this way is because the applications are the external tools that determine how to deliver critical information consumed from UICDS to computers in EOCs to a PDA or a smart cellular phone, even to a radio through digital voice.

UICDS cores can be deployed in a variety of peer-to-peer configurations (figure 3). The state emergency operations center or regional EOCs, may be supported by a multi-server UICDS installation that could support 1,000 or more application users with UICDS services, connecting to numerous external systems and recording and storing transactions from multiple incidents.

Local EOCs may operate UICDS on a single server or even on a desktop computer that could support 500 to 1,000 users, who would be interconnected to local responder applications but who would also use UICDS services and data storage for multiple smaller emergencies and daily operations. A local department or station (police, fire, emergency medical, etc.) could run a desktop computer, a few interconnected external applications, and department-specific storage responsibilities handling on the order of 300 to 500 end-users.

Finally, local agencies or mobile command vehicles would have a UICDS core, one or two interconnections to local applications, and limited storage, perhaps supporting 50 to 100 users, many on wireless devices.

Cores can be installed on virtually any server and network depending on the governance and policies of the participating organizations. Cores can be hosted by a government agency for several other agencies, or even a state for many of its jurisdictions. Core hosting can even be outsourced for those pilot sites that do not have the information technology infrastructure locally.

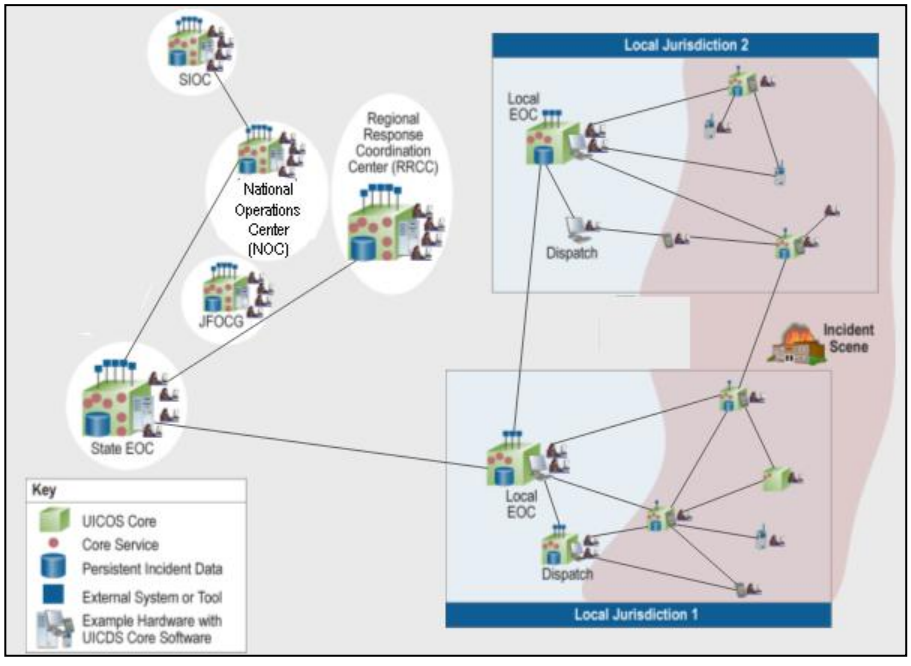

Figure 3. UICDS deployments connect diverse agencies in a peer-to-peer relationships and support applications that deliver UICDS information across a wide range of devices from a responder's PDA to vehicles to mobile command, small agencies, cities, counties, and statewide implementations. (SIOC = Strategic Information and Operations Center)

VII. Technology Applications from Industry, Government, and Academe

As middleware, UICDS does not interface directly with end users. Rather, it relies on regular, daily-use external applications as the source of and visualization for relevant data. UICDS is the transporter of uniform data in common formats. External applications (sensors, incident logs, personnel management, dispatch systems, video surveillance, and intelligence tools – anything related to homeland security) provide a portion of their data to UICDS, which then publishes it to subscribers' external applications. The external applications then visualize the consumed data inside their own user interface. Thus, to the user, there is no new application, no new learning, and no conscious sending of information.

As Chris Doyle said about UICDS and the "early adopter" technology providers at one of many UICDS reference implementation demonstrations: "Looking at it from an industry perspective, UICDS is not competing with industry. UICDS welcomes them into the fold so that the things they develop have an intended purpose and a match on the user side. These were the motivating factors in initiating these efforts in the first place.

"Whether we are talking about crossing domains or crossing roles or crossing whatever, fill in the blank, the objective of UICDS is to create a target for solution developers to aim for and I am very appreciative to all of our industry partners who have agreed to … to participate in this and kick the tires on this capability."

Larry Skelly, Deputy Director of the Infrastructure and Geophysical Division, describes the UICDS business model as: "The approach of UICDS is to go to the commercial vendors and explain the market potential for them to participate. And show them the value of the UICDS software development kit, which I think of as Velcro™. The software development kit essentially allows commercial developers to put one side of Velcro™ into their applications. We are not doing anything to their application. It is a black box to us. But we are letting them put Velcro™ on the side so that when that data owner wants to share with the UICDS core, the two can come together and hook up. This creates value for the commercial application and for the government end user."

Figure 4. Chris Doyle, Director of the Infrastructure and Geophysical Division, on why DHS S&T wanted to create UICDS: "What was needed was the ability to link existing legacy systems, because one of the things the Department needed to do was acknowledge that there had been significant investments already made at the state and local level in systems. Not only financial investments but time for people to learn these systems and become familiar with them and comfortable with them. So scrapping systems to build new ones to satisfy some federal requirement of HSPD-5 was not an option. Development of an architectural framework that acknowledges these differences in solutions that were already employed and would not require pulling the plug on those."

As of August 2010, more than 300 companies are engaged in dialogue about UICDS. More than 150 have signed up for the UICDS Development Kit. And over the course of the past two years, more than 40 applications had built adapters with the at the UICDS Development Kit to participate in demonstrations and pilots.

VIII. How to Participate in UICDS

The current program phase of UICDS continues to be supported by the Department of Homeland Security, Directorate of Science and Technology, Infrastructure and Geophysical Division. This phase will result in the piloting of UICDS in more than 100 locations in more than 25 states.

Pilot areas are selected by DHS to represent the type of deployments that will occur across the country in full implementation. These range from a city that wants to share information among its agencies, to city-to-city sharing, to city-to-county sharing, county-to-state, state-to-state, regional, federal, and military to civilian.

A pilot consists of a number of steps beginning with assessing information sharing requirements of the pilot area. This leads to identifying applications and agencies across jurisdictions that can participate in information sharing. Coordinating the establishment of information sharing agreements among all the participants leads to installing the UICDS Core(s) on a host network. An important step shared between the UICDS implementation organization and the pilot agencies is working with the Technology Providers to create and implement UICDS adapters. Throughout the pilot, UICDS operates daily and at least once an information sharing demonstration is conducted for the purpose of testing the implementation and promoting to neighboring organizations their participation in the UICDS pilot.

The goal of the pilot is to have the pilot area agencies request that DHS leave the complete UICDS installation at the conclusion of the pilot for the agencies to employ into the future for their own operational purposes.

The UICDS pilot is ongoing and can be initiated by either a government jurisdiction or a UICDS Technology Providers. To learn more and participate in a UICDS Pilot contact:

- James W. Morentz, Ph.D., director of UICDS Outreach at morentzj@saic.com
- Or you can register on the UICDS website at www.UICDS.us.