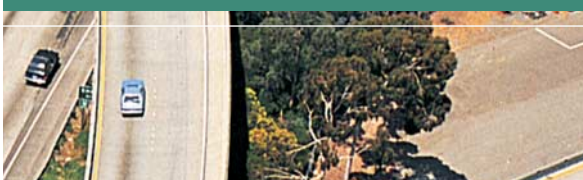
NCHRP
REPORT 525



Surface Transportation Security
Volume 2

Information Sharing and Analysis Centers: Overview and Supporting Software Features

TRANSPORTATION RESEARCH BOARD
OF THE NATIONAL ACADEMIES

NATIONAL COOPERATIVE HIGHWAY RESEARCH PROGRAM

NCHRP REPORT 525

Surface Transportation Security

Volume 2

Information Sharing and Analysis Centers: Overview and Supporting Software Features

JOHN N. BALOG
PETER N. BROMLEY
DAN DATTILIO
JAMIE BETH STRONGIN
McCORMICK, TAYLOR & ASSOCIATES, INC.
Philadelphia, PA

AND

ANNABELLE BOYD
JIM CATON
ANDREW LOFTON
BOYD, CATON & GRANT TRANSPORTATION GROUP, INC.
Charlottesville, VA

SUBJECT AREAS
Planning and Administration • Energy and Environment • Transportation Law

Research Sponsored by the American Association of State Highway and Transportation Officials
in Cooperation with the Federal Highway Administration

TRANSPORTATION RESEARCH BOARD

WASHINGTON, D.C.
2004
www.TRB.org

NATIONAL COOPERATIVE HIGHWAY RESEARCH PROGRAM

Systematic, well-designed research provides the most effective approach to the solution of many problems facing highway administrators and engineers. Often, highway problems are of local interest and can best be studied by highway departments individually or in cooperation with their state universities and others. However, the accelerating growth of highway transportation develops increasingly complex problems of wide interest to highway authorities. These problems are best studied through a coordinated program of cooperative research.

In recognition of these needs, the highway administrators of the American Association of State Highway and Transportation Officials initiated in 1962 an objective national highway research program employing modern scientific techniques. This program is supported on a continuing basis by funds from participating member states of the Association and it receives the full cooperation and support of the Federal Highway Administration, United States Department of Transportation.

The Transportation Research Board of the National Academies was requested by the Association to administer the research program because of the Board's recognized objectivity and understanding of modern research practices. The Board is uniquely suited for this purpose as it maintains an extensive committee structure from which authorities on any highway transportation subject may be drawn; it possesses avenues of communications and cooperation with federal, state and local governmental agencies, universities, and industry; its relationship to the National Research Council is an insurance of objectivity; it maintains a full-time research correlation staff of specialists in highway transportation matters to bring the findings of research directly to those who are in a position to use them.

The program is developed on the basis of research needs identified by chief administrators of the highway and transportation departments and by committees of AASHTO. Each year, specific areas of research needs to be included in the program are proposed to the National Research Council and the Board by the American Association of State Highway and Transportation Officials. Research projects to fulfill these needs are defined by the Board, and qualified research agencies are selected from those that have submitted proposals. Administration and surveillance of research contracts are the responsibilities of the National Research Council and the Transportation Research Board.

The needs for highway research are many, and the National Cooperative Highway Research Program can make significant contributions to the solution of highway transportation problems of mutual concern to many responsible groups. The program, however, is intended to complement rather than to substitute for or duplicate other highway research programs.

Note: The Transportation Research Board of the National Academies, the National Research Council, the Federal Highway Administration, the American Association of State Highway and Transportation Officials, and the individual states participating in the National Cooperative Highway Research Program do not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the object of this report.

NCHRP REPORT 525: Volume 2

Project 20-59(10) FY'03

ISSN 0077-5614

ISBN 0-309-08803-8

Library of Congress Control Number 2004111186

Price $28.00

NOTICE

The project that is the subject of this report was a part of the National Cooperative Highway Research Program conducted by the Transportation Research Board with the approval of the Governing Board of the National Research Council. Such approval reflects the Governing Board's judgment that the program concerned is of national importance and appropriate with respect to both the purposes and resources of the National Research Council.

The members of the technical committee selected to monitor this project and to review this report were chosen for recognized scholarly competence and with due consideration for the balance of disciplines appropriate to the project. The opinions and conclusions expressed or implied are those of the research agency that performed the research, and, while they have been accepted as appropriate by the technical committee, they are not necessarily those of the Transportation Research Board, the National Research Council, the American Association of State Highway and Transportation Officials, or the Federal Highway Administration, U.S. Department of Transportation.

Each report is reviewed and accepted for publication by the technical committee according to procedures established and monitored by the Transportation Research Board Executive Committee and the Governing Board of the National Research Council.

To save time and money in disseminating the research findings, the report is essentially the original text as submitted by the research agency. This report has not been edited by TRB.

Published reports of the

NATIONAL COOPERATIVE HIGHWAY RESEARCH PROGRAM

are available from:

Transportation Research Board
Business Office
500 Fifth Street, NW
Washington, DC 20001

and can be ordered through the Internet at:

http://www.national-academies.org/trb/bookstore

Printed in the United States of America

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. On the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Bruce M. Alberts is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. William A. Wulf is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, on its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both the Academies and the Institute of Medicine. Dr. Bruce M. Alberts and Dr. William A. Wulf are chair and vice chair, respectively, of the National Research Council.

The **Transportation Research Board** is a division of the National Research Council, which serves the National Academy of Sciences and the National Academy of Engineering. The Board's mission is to promote innovation and progress in transportation through research. In an objective and interdisciplinary setting, the Board facilitates the sharing of information on transportation practice and policy by researchers and practitioners; stimulates research and offers research management services that promote technical excellence; provides expert advice on transportation policy and programs; and disseminates research results broadly and encourages their implementation. The Board's varied activities annually engage more than 5,000 engineers, scientists, and other transportation researchers and practitioners from the public and private sectors and academia, all of whom contribute their expertise in the public interest. The program is supported by state transportation departments, federal agencies including the component administrations of the U.S. Department of Transportation, and other organizations and individuals interested in the development of transportation. **www.TRB.org**

www.national-academies.org

COOPERATIVE RESEARCH PROGRAMS STAFF FOR NCHRP REPORT 525 VOLUME 2

ROBERT J. REILLY, *Director, Cooperative Research Programs*
CRAWFORD F. JENCKS, *Manager, NCHRP*
S. A. PARKER, *Senior Program Officer*
EILEEN P. DELANEY, *Director of Publications*
HILARY FREER, *Editor*
BETH HATCH, *Assistant Editor*

NCHRP PROJECT SP20-59
Field of Special Projects—Area of Security

DAVID DEO LARSON, *Wisconsin DOT* (Chair)
DAVID P. ALBRIGHT, *New Mexico Office of Homeland Security, Santa Fe, NM*
CHARLES CARR, *Mississippi DOT*
WILLIAM J. FLEMING, *Massachusetts Bay Transportation Authority, Boston, MA* (retired)
ADAM GOLODNER, *Dartmouth College*
THOMAS HICKS, *Maryland State Highway Administration*
VINCENT P. PEARCE, *FHWA*
RAY L. PURVIS, *Missouri DOT* (retired)
THOMAS RUMMEL, *Texas DOT*
DOTTIE SHOUP, *Nebraska DOR*
TERRY SIMMONDS, *Washington State DOT* (retired)
JOHN GERNER, *FHWA Liaison Representative*
ROBERT D. JAMISON, *FTA Liaison Representative*
THEOPHILOS C. GEMELAS, *DHS TSA Liaison Representative*
DAVID S. EKERN, *AASHTO Liaison Representative*
ANTHONY R. KANE, *AASHTO Liaison Representative*
GREG HULL, *APTA Liaison Representative*
JANET K. BENINI, *USDOT Research and Special Programs Administration Liaison Representative*
PAUL GOLDEN, *DHS Infrastructure Coordination and Analysis Office - ISAC Development & Support Unit Liaison Representative*
JOHN HARRIS, *DHS TSA Liaison Representative*
MATTHEW D. RABKIN, *USDOT Volpe National Transportation Systems Center Liaison Representative*
IAN A. REDHEAD, *Airports Council International-North America Liaison Representative*
TOM SACHS, *USDOT Research and Special Programs Administration Liaison Representative*
SUSAN I. SMITH, *FBI Liaison Representative*
JOEDY W. CAMBRIDGE, *TRB Liaison Representative*

FOREWORD

By S. A. Parker
Staff Officer
Transportation Research Board

This second volume of *NCHRP Report 525: Surface Transportation Security* will be of interest to those responsible for analyzing intelligence to determine threats to transportation assets; included will be chief executive officers, senior executives, operational and technical managers, law enforcement officers, security personnel, and communications and human-resources staff. Personnel with similar responsibilities in public transportation or public works will also find this report to be of value. The objective of *Volume 2: Information Sharing and Analysis Centers: Overview and Supporting Software Features* is to provide background for decisions on how to organize and share security threat information across transportation organizations. McCormick Taylor, Inc., prepared this volume of *NCHRP Report 525* under NCHRP Project 20-59(10).

Emergencies arising from terrorist threats highlight the need for transportation managers to minimize the vulnerability of travelers, employees, and physical assets through incident prevention, preparedness, response, and recovery. Managers are seeking to reduce the chances that transportation vehicles and facilities will be targets or instruments of terrorist attacks and to be prepared to respond to and recover from such possibilities. By being prepared to respond to terrorism, each transportation agency is simultaneously prepared to respond to natural disasters such as hurricanes, floods, and wildfires, as well as human-caused events such as hazardous materials spills and other incidents.

This is the second volume of *NCHRP Report 525: Surface Transportation Security*, a series in which relevant information is assembled into single, concise volumes—each pertaining to a specific security problem and closely related issues. These volumes focus on the concerns that transportation agencies are addressing when developing programs in response to the terrorist attacks of September 11, 2001, and the anthrax attacks that followed. Future volumes of the report will be issued as they are completed.

To develop this volume in a comprehensive manner and to ensure inclusion of significant knowledge, available information was assembled from numerous sources, including a number of state departments of transportation. A topic panel of experts in the subject area was established to guide the researchers in organizing and evaluating the collected data and to review the final document.

This volume was prepared to meet an urgent need for information in this area. It records practices that were acceptable within the limitations of the knowledge available at the time of its preparation. Work in this area is proceeding swiftly, and readers are encouraged to be on the lookout for the most up-to-date information.

Volumes issued under *NCHRP Report 525: Surface Transportation Security* may be found on the TRB website at http://www4.trb.org/trb/crp.nsf/All+Projects/NCHRP+20-59.

CONTENTS

EXECUTIVE SUMMARY

There is a need on the part of the state departments of transportation (DOTs) to communicate in a secure manner internally within their own departments, spread out within state boundaries and with other state DOTs, the Federal Highway Administration (FHWA), the Federal Emergency Management Agency (FEMA) and other federal agencies within the Department of Homeland Security (DHS) as well as other federal agencies, law enforcement, and emergency responders. While this need has likely been present for some time, the impetus for its most recent drive has been the horrific terrorist actions in the fall of 2001.

Underlying this concept of a secure communications system has been the strong belief that the state DOTs had information which could be mutually beneficial if shared and which might amount to a pattern discernable to counter-terrorist analysts, were it properly collected, sorted and analyzed, or data mined.

At the same time, the states are aware both of the limited budgets and daunting tasks currently before most state DOTs. While security has always been a concern, the events of 2001 have raised the stakes and the relative priority of security in the array of tasks which the DOTs must daily undertake. The results of this research effort have revealed, if it were ever in doubt, that communicated security threats (not even to speak of bona fide security threats) are, in most cases, a reasonably rare though clearly critical occurrence. State budgets and the responsibilities and tasks of state DOTs being what they are, there has been a belief that perhaps a secure communication system which served the states in the area of transportation security could also serve in times of other, natural emergency events such as approaching hurricanes, blizzards or wildfires.

INTEGRATED TRANSPORTATION ANALYSIS (ITA) SYSTEM DEMONSTRATION

This research effort to make a secure, national communication infrastructure began in late June of 2002 with a nationwide test of the competency of a new secure communication system, called the Integrated Transportation Analysis (ITA) system. The ITA system was initially a cooperative venture primarily involving the New Mexico State Highway and Transportation Department (NMSHTD) and Sandia National Laboratories (Sandia). The ITA system was designed to serve as a communication device that would allow real-time posting and communication of actual information on natural and intentional emergencies for distribution among states and other agencies including the federal government and law enforcement agencies. To the knowledge of the Research Team at that time, no other such system existed which could occupy the same critical function. Indeed, throughout this research effort, it has been clear that the role and capabilities of the ITA system are unique.

The demonstration highlighted that the communication aspects of the ITA system are more fully developed than the analytical aspects. The demonstration of the ITA system on July 3, 2002 was primarily designed to evaluate whether four communication competencies could be established. Competencies associated with the analytical capabilities were not tested.

In the judgment of the McCormick, Taylor & Associates Team of observers, the four minimum core communication competencies, desired and claimed before the demonstration, were established during the demonstration, at least in a limited application. The ability for individuals to call into the Call Center to convey the presence of a threat, and to distribute this and follow-up messages in a secure manner via a Virtual Private Network (VPN) to the five participating states and the seven other agencies including the FBI and the US Department of Transportation (USDOT) was successful.[1] In addition, the ability to use a secure website as a repository for all communications and to use the geographic information systems (GIS) to display information necessary to develop and effect a response to an incident was established.

At the same time, the ability of the ITA system operational prototype to act reliably in a sustained manner was not proven at the demonstration. It should be noted that reliability and sustainability issues are technical concerns that can be expected to be resolved in the future and were not targeted as competency areas. Unfortunately, the reliability and sustainability attributes were troublesome enough during the demonstration to detract from the fact that the four targeted competencies were established.

It should be noted that the ITA system currently offers considerable value to all potential users. The demonstrated version of the ITA system was proven to offer considerable conceptual capability regarding the needs of the transportation industry.

NATIONWIDE SUMMIT ON SECURE COMMUNICATION INFRASTRUCTURE FOR TRANSPORTATION INDUSTRY EMERGENCIES

From the nationwide demonstration of the ITA system, the research effort ventured toward establishing functional specifications for a secure communications infrastructure by means of the convening of a nationwide summit of transportation security experts held in Washington, D.C. on February 20–21, 2003.

Summit participants conveyed the message that a variety of users and user groups should be considered for a secure communication system. These users would be responsible for the housing, operation, and maintenance of such a system.[2] The following suggested users were identified at the Summit:

---

[1] Participants in the ITA system demonstration were the United States Department of Transportation (US DOT), Transportation Information and Operations Center (TIOC), in the District of Columbia; Maryland State Highway Administration (MDSHA), near Baltimore, Maryland; Texas Department of Transportation (TXDOT), in Austin, Texas; Washington State Department of Transportation (WSDOT), in Olympia, Washington; Federal Bureau of Investigation (FBI), National Infrastructure Protection Center (FBI-NIPC) in Washington, DC; United States Department of Transportation, Federal Highway Administration (FHWA) District Office in Texas; New Mexico State Highway and Transportation Department (NMSHTD) General Office; the FHWA District Office in New Mexico, NMSHTD District Six in Grants/Milan, New Mexico; the Albuquerque Call Center site at the New Mexico State Police (NMSP); the New Mexico State Emergency Management Center; the Albuquerque Field office of the FBI; the Sandia National Laboratory.

[2] However, it was not clearly defined during this specific session how all of these entities would be integrated together into a coherent and functional system. Some of these points are addressed later in this document.

- ❒ first responders;
- ❒ first person(s) on the scene (highways, transit);
- ❒ traffic operations centers;
- ❒ state Highway Patrol, police or equivalent;
- ❒ National Guard;
- ❒ state emergency divisions or departments;
- ❒ the Surface Transportation Information Sharing and Analysis Center (ST-ISAC);
- ❒ public transportation systems;
- ❒ private industry—bus companies, highway freight, rail freight, bridges and tunnels, turnpikes, school buses, ports, ferry systems;
- ❒ Department of Defense;
- ❒ US DOT and particularly, the Crisis Management Center (CMC);
- ❒ Department of Homeland Security (DHS);
- ❒ American Bus Association (ABA);
- ❒ State DOTs;
- ❒ American Association of State Highway and Transportation Officials (AASHTO);
- ❒ American Public Transportation Association (APTA);
- ❒ Community Transportation Association of America (CTAA);
- ❒ Canadian Urban Transit Association (CUTA);
- ❒ Bridge and Tunnel Owners Association;
- ❒ Border Patrol and Immigration;
- ❒ Canada;
- ❒ Mexico;
- ❒ local DOTs;
- ❒ general aviation;
- ❒ other Information Sharing and Analysis Centers (ISACs);
- ❒ American Public Works Association (APWA);
- ❒ National Association of County Engineers (NACE); and
- ❒ American Trucking Association (ATA).

The length of this list was surprising since the basic, first goal of the secure communication system as originally expressed was to connect state departments of transportation and a reasonable group of first responders and other partners necessary to identify and respond to an emergency or terrorist threat. The length and breadth of this expressed user community would raise the technical, practical and security complexities substantially.

It was determined during the Summit that the secure communication system would need to fully satisfy many roles or functions, including information collection and sharing, as well as real or near time data analysis, event prediction, and data mining. One concern of some Summit participants was to what extent the data would be analyzed and sorted by the administration system before it reached the end user. Would it be filtered before it would be sent out, or would it simply be presented as raw data? If no sorting takes place prior to submittal, who would be responsible for sifting through this raw data? This set of questions drives the concept as to how fast the data is made available, whether in real time, near time, or lagged time and how it may be used once it is received.

Questions regarding who would own the system came up quite frequently. Many suggestions regarding ownership were made, including:

- ❒ government (owned by the US DOT);
- ❒ quasi-government;
- ❒ non-profit advocacy organization (such as AASHTO or APTA);
- ❒ private organization;
- ❒ newly formed limited liability corporation (LLC);
- ❒ ST-ISAC; and/or
- ❒ a combination of all of these.

Legal implications were briefly discussed. Many agreed that a limited liability corporation (LLC) would minimize the liability of state DOTs, AASHTO or any other construct. However, private ownership could result in a difficult situation, should the owner need to file for bankruptcy or wish to exit the role as a result of inadequate rate of return on its investment. Representative experts at the Summit agreed that liability would need to be minimized in order to allow for acceptance of a communication system by state DOTs that could be owned, maintained, and administrated by AASHTO. Furthermore, the legal effects on the organization controlling access to such a system would also need to be minimized.

A unanimous recognition that occurred at the conclusion of the Summit concerned continuity. Participants stated that a long-term funding stream and federal commitment (including AASHTO support) would be imperative to the successful implementation of a secure communication system. It was clear that the states believed that federal funding was necessary to support the deployment, maintenance, administration, and timeliness of the secure communication system. Many agreed that a funding model would need to be presented and agreed upon if the concept were to be correctly implemented.

Discussions of *Interoperability* and *Standards* yielded suggestions for an open architecture with redundant systems. However, many agreed that while systems should be redundant to maximize their availability, the information they receive, process, and distribute should not be. This is particularly true regarding how many times the same information would have to be entered. Obviously, it is important to design a system that requires only one insertion of primary data; every time data is reentered, the potential for errors increases and in a busy operating environment, provokes frustration and disuse. This causes compatibility problems. Therefore, a secure communication network should be made to minimize the redundancy of information input by the operator, user, or the software itself.

It was apparent from the Summit that key steps will need to be considered in initiating a secure communications network. These steps will deal with the policy, process, and procedures directly affecting the system, as well as the actual design of software technology and training of the system users. In managing the information transmitted over the network, four basic questions will need to be answered. These are as follows.

- ❒ What do you do with it?
- ❒ How do you use it?

- ❒ What do you report?
- ❒ How do you report it?

NATIONAL SURVEY OF STATE DEPARTMENTS OF TRANSPORTATION

Shortly after the Summit concluded, the Research Team administered a nationwide survey on transportation security through the state DOTs. Twenty-eight jurisdictional entities responded.[3]

State DOT respondents described their need for an information sharing system that brings local information from a variety of transportation, law enforcement, and public health agencies to their attention and, likewise, enables them to share threats and warnings with other state DOTs and with the federal government.

State DOTs indicated that the implemented secure communication system should support planning, preparedness, and response, though its primary function is to relay threats and warnings.

While state DOTs would like more information from a range of agencies, it appears that the greatest need is for information from other state DOTs and the federal government.

The majority of respondents have an employee awareness program and existing procedures have been modified to address the reporting and investigation of potential security threats and incidents.

Since 2000, state DOT respondents have experienced an increasing number of threats and performed an increasing number of serious investigations regarding potential security incidents.

State DOTs, while expressing an interest in information sharing with a multitude of agencies, also indicated their preference for focused, verified and analyzed threat information. A majority of state DOTs indicated a preference that the secure communication system would provide some degree of filtering of information, and also, perhaps, prioritization of threat severity to support management of what could potentially be an overwhelming amount of information.

State DOTs have limited experience with existing threat and warning systems and limited resources with which to pursue these systems. Though 64 percent of survey respondents indicated that they would pay a users fee for access to a secure communications system, there appears to be a consensus regarding the need for federal funding to support (or at least initiate) the system.

[3] The survey was sent to all 50 states and the District of Columbia.

State DOTs have different responsibilities for multiple modes of transportation. State DOTs also play key roles during the activation of the State Emergency Operations Plan, which relies on their connections across multiple modes and services. The secure communications system should preserve access to as much multi-modal information as possible.

FEATURES CATALOGUE

Partially in response to the results of the Summit and the survey, the research effort sought to compare existing communications packages which might be used by the states. The results of this effort, the Features Catalogue, is presented in the next section of this report and summarizes the descriptive features associated with a specifically selected set of secure communication information systems thought to be similar with respect to their potential ability to support state DOTs in the receipt of threat and other information, the processing of the received information, and the administration and tracking of any implemented response activities. The reported information in this section is primarily based on the results of personal interviews and other interactions with developers and end-users of the selected systems. Features associated with the following seven systems are included in this report:

- ❒ Activation Information Management (AIM);
- ❒ Disaster Management Interoperability Services (DMIS);
- ❒ InfraGard;
- ❒ Integrated Transportation Analysis (ITA);
- ❒ Intelligent Road and Rail Information Server (IRRIS);
- ❒ MobileShield™; and
- ❒ Surface Transportation Information Sharing and Analysis Center (ST-ISAC).

Twenty-three interactions with the key developers and typical end-users of these systems were conducted during the period from May through July of 2003. These contacts appear in Appendix E of this report.

In addition, three other related software system programs are briefly described in this section which may also have some direct relevance to the needs of the state DOTs. The information on these systems was primarily taken from open sources; no interviews of developer or end-user professionals associated with the programs were completed, nor were any direct contacts with such professionals made. These three additional programs were:

- ❒ Global Justice Information Sharing Initiative (Global);
- ❒ Organization for the Advancement of Structured Information Services (OASIS); and
- ❒ Regional Information-Sharing Systems (RISS).

It is suggested that each state DOT and other interested parties may use the information in this section as a starting or reference point in the process to select the software system(s) considered to be potentially most useful in satisfying their local needs. It should also be

recognized that there might be additional software systems that were not catalogued or described as part of this research Task Order that may prove useful to state DOTs.[4]

Two user-friendly matrixes regarding the features of the seven software systems identified above are provided to assist transportation decision-makers in selecting the secure communication system(s) that will appropriately satisfy their needs for information sharing: the Developer Features Matrix and the End-User Features Matrix.

It is strongly suggested that before any of these systems (or any other systems, for that matter) are acquired or purchased, they should be thoroughly tested by the potential user in their then current environment or a similar environment and that functional specifications regarding the actual capabilities of the desired software system be comprehensively developed and included in the procurement bid package used by the procuring agency. The information presented here is simply a snapshot of the selected systems at the point in time of the data collection process and no verification of the acquired information or testing of the systems was accomplished as part of the requirements of the statement of work associated with this Task Order. Thus, no warranty regarding the functional and operational capabilities of any of the systems can be either expressed or implied.

INFORMATION SHARING AND ANALYSIS CENTERS (ISACS)

The research effort also explored the subject of an Information Sharing and Analysis Center (ISAC) for the highway transportation sector. This discussion is presented after the Features Catalogue.

With the issuance of Presidential Decision Directive 63 (PDD-63) by President Clinton in 1998 came a new concept that each industry critical to the national infrastructure should assume significant responsibility for contributing to its own protection. Through this Directive, a number of industries established their own formalized programs of networks and systems for secure information identification and exchange. These became known as Information Sharing and Analysis Centers (ISACs).

The critical industry sectors originally identified by PDD-63 as benefiting from the potential value of an ISAC were:

- ❒ information and communications;
- ❒ electric power;
- ❒ gas and oil production and storage;
- ❒ banking and finance;
- ❒ transportation;
- ❒ water supply;
- ❒ emergency services; and
- ❒ government services.

[4] The seven software systems comprehensively considered in this section were identified initially as part of earlier work on this Task Order in addition to those suggested by members of the NCHRP Panel.

Additional industries have since adopted the ISAC concept and are currently building their own networks and systems for secure information identification and exchange. These critical industry sectors are:

- ❒ food;
- ❒ chemicals; and
- ❒ interstate.

The first ISAC, the Financial Services ISAC (FS-ISAC), became initially functional in October 1999 by focusing primarily on the establishment of reliable security for the cyber activities of its membership. As additional ISACs were created with significant concerns for information systems and a variety of cyber security forms, the intent of the ISAC industry began to expand and mature with additional attention being directed toward physical protection, particularly in recent years.

Once created, no industry's ISAC has been terminated or has withdrawn from support of its stated goals. The practice of establishing networks and systems for secure information identification and exchange among industry leaders has now been in place for nearly four years. This indicates that many critical infrastructure industries have recognized the inherent value and usefulness of a tailored ISAC. However, an ISAC can only be fully functional if it is supported by its membership, the practitioners within its industry sector.

The transportation industry has responded to the challenge exhibited in PDD-63 by creating standalone ISACs to facilitate the secure exchange of information throughout its many specialized sectors, including rail freight and trucking within the surface transportation area, and aviation in a separate endeavor. The public transportation industry has chosen to become associated with the Surface Transportation ISAC (ST-ISAC), with the American Public Transportation Association (APTA) serving as a Sector Coordinator.

This section takes a close look at the concerns that need to be considered in establishing an ISAC.

FEATURES CATALOGUE

INTRODUCTION

The collection and tabulation of information on secure threat identification, response and tracking communication systems was a logical follow on to previous activities associated with this Task Order. The first activity was to functionally and operationally evaluate selected competencies of the Integrated Transportation Analysis (ITA) System[1] during a real time implementation test involving five state departments of transportation (state DOTs), the US Department of Transportation, and the Federal Bureau of Investigation (FBI), among other related transportation entities. The results of this activity were reported in:

- *Preliminary Draft Final Report, Evaluation of the July 3, 2002 Integrated Transportation Analysis (ITA) System Demonstration*.[2]

In the second major activity associated with this Task Order a summary of a survey of the secure communication needs of the state DOTs, and a summary of a Nationwide Summit on Secure Communication Infrastructure for Transportation Emergencies was produced. The results were reported in:

- *Preliminary Draft Final Report, Secure Communication Infrastructure, Phases 2 and 3, Task 4A*.[3]

This Preliminary Draft Final Report (PDFR) summarizes the features of a number of potentially useful software systems in matrix form, based on the content of interviews and interactions conducted with the developers and selected end-users of the products. The systems catalogued were initially identified during the earlier activities of the Task Order and were augmented with those suggested by members of the National Cooperative Highway Research Program (NCHRP) Panel. While all the investigated software systems initially appeared to offer significant capabilities for the receipt of threat and other information, the processing of the received information, and the administration and tracking of any implemented response activities, the collected data reveals considerable variation regarding

---

[1] Sandia National Laboratories and the New Mexico Department of Highways and Transportation jointly developed the ITA system that was evaluated.

[2] Balog, John N.; Bromley, Peter N.; Strongin, Jamie Beth; Dattilio, Daniel J.; Boyd, Annabelle; and Caton, James, *Preliminary Draft Final Report: Evaluation of the July 3, 2002 Integrated Transportation Analysis (ITA) System Demonstration, NCHRP Project 20-59(10)*, McCormick, Taylor & Associates, Inc., National Cooperative Highway Research Program, Transportation Research Board, Washington, DC, July 22, 2002. Much of this material is found in Appendix A of this report.

[3] Balog, John N.; Boyd, Annabelle; Bromley, Peter N.; Caton, James; Dattilio, Daniel J.; and Strongin, Jamie Beth; *Secure Communication Infrastructure Phases 2 and 3, Task 4A, Preliminary Draft Final Report on Tasks 1 and 2*, NCHRP Project 20-59(10), McCormick, Taylor & Associates, Inc., National Cooperative Highway Research Program, Transportation Research Board, Washington, DC, March 10, 2003.

the capability and applicability to the potential requirements of state DOT and related transportation entity needs. It is believed that the content of the matrixes will serve as a starting or reference point as state DOTs and others pursue a decision regarding the secure communication system or systems that are most appropriate to their needs. Indeed, it may be most appropriate for some state DOTs to actually acquire and implement more than one system in order to achieve all of their goals. However, it appears from much of the discussion that occurred at the Summit, and from the results of the survey of the state DOTs, that many states are interested in being able to use the ultimately selected and implemented software system(s) as a basis for efficient and effective communication among each other. So, this consideration may be an overriding influence in the selection process. The information presented in this report is expected to be able to contribute to the decision-making process of the state DOTs and other transportation entities. It should be noted that other systems may also be available that satisfy some or many local needs that have not been catalogued here. However, it is believed that the reviewed systems are a reasonable indication of the status of the available marketplace.

Features associated with the following seven systems consistent with the identified focus of the research are included in this report:

- ❒ Activation Information Management (AIM);
- ❒ Disaster Management Interoperability Services (DMIS);
- ❒ InfraGard;
- ❒ Integrated Transportation Analysis (ITA);
- ❒ Intelligent Road and Rail Information Server (IRRIS);
- ❒ MobileShield™; and
- ❒ Surface Transportation Information Sharing and Analysis Center (ST-ISAC).

These systems were selected as a logical follow-on to the earlier activities of this Task Order, and include systems recommended for consideration by members of the National Cooperative Highway Research Program Panel.

In addition, the following three additional programs are briefly described to illustrate their potential application in contributing to the satisfaction of state DOT needs:

- ❒ Global Justice Information Sharing Initiative (Global);
- ❒ Organization for the Advancement of Structured Information Services (OASIS); and
- ❒ Regional Information-Sharing Systems (RISS).

ORGANIZATION OF THE FEATURES CATALOGUE

This Features Catalogue has been partitioned into the following subsections.

- ❒ Introduction. This subsection provides an overview of the Features Catalogue by discussing the characteristics of the research program applied to this Task Order.

- Descriptions. Each of the seven highlighted secure communication systems is more thoroughly discussed in this subsection. These systems are:
  - Activation Information Management (AIM);
  - Disaster Management Interoperability Services (DMIS);
  - InfraGard;
  - Integrated Transportation Analysis (ITA);
  - Intelligent Road and Rail Information Server (IRRIS);
  - MobileShield™; and
  - Surface Transportation Information Sharing and Analysis Center (ST-ISAC).

- Matrix Description. This subsection outlines the organization and methodology of the Features Matrix.

- Features Matrix. This subsection is partitioned into two primary elements entitled Developer Features Matrix and End User Features Matrix. These in-depth matrixes are comprised of the detailed questions posed to the interviewees. The responses of the interviewed developers and end-users and other submissions are included in the matrixes.

- Three Additional Systems for Consideration. At the *Summit on Interoperable Communications for Public Safety*[4] on June 26–27, 2003, approximately 60 communication systems were presented and discussed. Of these, three systems seemed to lend themselves to the application of secure communication within the transportation industry. Information on these systems, taken from the published Briefing Book and from respective open source websites is included in this subsection. Since interviews were not conducted with the developers and end-users of these software systems, the matrixes used to report the results of the interviews of the systems identified in the earlier subsection are not used here. These additional systems are:
  - Global Justice Information Sharing Initiative (Global);
  - Organization for the Advancement of Structured Information Services (OASIS); and
  - Regional Information Sharing Systems (RISS).

- Interviewed and Contacted Developers and End-Users. Appendix E of this report provides a complete listing of the developers and end-users that were interviewed, either in-person or contacted over the telephone.

[4] Department of Commerce, National Institute of Standards and Technology, Office of Law Enforcement Standards; Department of Justice, National Institute of Justice, AGILE Program; and Department of Homeland Security, Science and Technology Directorate, SAFECOM, *Briefing Book of Public Safety Related Groups and Programs on Interoperable Communications and Information Sharing*, Summit on Interoperable Communications for Public Safety, Office of Management and Budget, Washington, DC, June 26–27, 2003.

DEFINING THE SCOPE OF THE RESEARCH

At the Nationwide Summit on Secure Communication Infrastructure for Transportation Industry Emergencies (Summit) held in February 2003, secure communication systems that were mentioned by key decision-makers within the transportation industry were noted and added to the previously developed list of potentially useful systems. The Integrated Transportation Analysis (ITA) system, which is primarily used to communicate threats and warnings to the transportation industry, had been previously and thoroughly reviewed[5] in Phase 1 of this Task Order with respect to a number of specific competencies. It is also included here because of its initial and continued relevance to this Task Order.

In this Features Catalogue, the reported information is rendered from direct interviews conducted with developers of the investigated software systems and their end-users, using the questions included in the matrixes. In contrast, the developers and one end-user of the ITA system were asked to fill out the matrixes themselves, and their submissions are for the most part a verbatim expression of the submitted information.[6] It should be noted that the information on the ITA system in the Developers Features Matrix is placed on two separate lines. The first line is the response received from the developer of the currently deployed prototype system. The second line is the response received from the developer of the proposed national system.

Key decision-makers at the Summit regarded many of these identified systems as being potentially useful to the transportation industry. While collecting the information on the identified systems, it was found that some of the systems are comprised of more functions related to consequence management than to communicating threats and warnings and to implementing and tracking immediate response actions. Incident or consequence management systems are certainly an asset to the industry. They can serve as excellent tools to conduct training simulations and drills or to help the industry mobilize with other emergency management personnel or agencies during an incident. However, many of these systems are not specifically designed to primarily communicate threats and warnings to their end-users. The ITA system differs from the others because it is intended to ultimately be able to provide a capability for predicting security-related events.

Cataloging of the consequence management systems was beyond the scope of work associated with this Task Order, though their capabilities are still viewed as relevant to the overall response programs being created by state DOTs, and may be included in the menu of capabilities selected for implementation by state DOTs and other related entities. In certain cases, consequence management systems can be linked to a communication software system designed to generate threat warnings. Nonetheless, the primary goal of this research was to investigate systems that would be appropriate for the states to

---

[5] Balog, John N. et al, *Preliminary Draft Final Report: Evaluation of the July 3, 2002 Integrated Transportation Analysis (ITA) System Demonstration*, *Op. Cit*.

[6] Spelling and grammatical errors, however, have been corrected and some additions were included to make the presentation of the ITA information consistent with that of the other systems.

use in communicating threats and other information between and among each other. Consequence management tools, by themselves, did not meet this criterion.

Whatever the state of the market for electronic emergency management tools prior to September 11, 2001, in the period after these terrible events, the market has been extremely expansive and competitive. There are many such products now available with, in some cases, quite persistent marketing programs. However, the products considered in this research were specifically chosen because of their expected value to the state DOTs. While software associated with managing emergency operations and the consequences of the emergency could assist a state DOT, the products sought for features cataloging were far more oriented toward the sharing of information, resources, threats and warnings in a secure manner. Most of the software associated with emergency management is oriented differently with perhaps one module devoted to communication of sensitive (not generally classified) information. The statement of work for this Task Order indicated that the state DOTs were primarily interested in a more robust product for secure communication. They also have interest in disaster management tools, but the identification and cataloging of such systems were beyond the current statement of work.

A relatively new, concerted effort to coordinate information from a variety of sources related to disaster management was also included within the systems considered. The basis of this inclusion was that all disaster-related software would, most likely, have to be compatible or made to be compatible with whatever system(s) the states might select for acquisition and implementation. Information was consequently collected on the Federal Emergency Management Agency's (FEMA)[7] efforts to produce seamless disaster management tools for the responder community. This system has been entitled the Disaster Management Interoperability Services (DMIS) suite.

SCOPE OF RESEARCH

Two forms for the collection of applicable information were developed, tested and applied. The first was the Developer Communication System Feature Data Form. This form contained space for the answers to 78 questions related to the design, features, implementation, training requirements and costs of secure communication software systems. A companion data form was also developed, tested and applied, the End-User Communication System Feature Data Form. This form contained 49 questions, intended for those currently using the respective systems, to indicate their actual experiences. Though these forms were also entitled questionnaires, a variety of methods were necessary to be employed for the collection of the appropriate information. In general, face-to-face interviews were conducted whenever possible. In some cases, the geography, limited timeframe, and finite budget did not allow for information to be collected in this manner, and telephone interviews were conducted. However, 10 of the interviews were administered on-site. These face-to-interviews proved beneficial to gaining valuable knowledge regarding the specific systems.

[7] FEMA is now part of the Department of Homeland Security.

Twenty-three total interviews and interactions were completed in order to populate the cells of the Features Matrixes.

It should be noted that not all systems were as developed and advanced as it may have initially been believed, based on the available published materials and word of mouth expressions.[8]

Certain developers of the software systems were less than fully cooperative in offering the names of appropriate users to interview or interact with, and this was a concern. However, it became understood that the experience of many current system users was limited to only short periods of time and thus some reluctance on the part of the developers to allow discussions with these users became apparent. In addition, given that threat occurrences for most transportation agencies appear to be fairly rare, even for systems that have longer periods of field experience, the frequency of threat and warning messages sent or received have generally not been great. Furthermore, not all end-users are currently able to develop their most-preferred configuration for their software system and, therefore, not all supporting systems are in place for a communication system to be completely operational.

As is apparent from an overview of the findings, the systems vary widely in their intended purposes, designs, emphases, and the uses for which they are currently employed. It should be recognized that it is not the intent of this catalogue to make a recommendation to the transportation community regarding what system(s) should be deployed. Rather, the intent is to provide comparable information on the identified systems so that each state DOT and other transportation entity decision-maker can use the provided input as part of its local evaluation process. It is likely that there is no perfect system available to completely satisfy all potential users, and depending on one's perspective, a positive case could be made for any of the system's catalogued.

It is strongly urged that before any of these systems are acquired or purchased they should be thoroughly tested by the potential user in their then current environment or a similar environment and that functional specifications regarding the actual capabilities of the desired software system be comprehensively developed and included in the procurement bid package used by the procuring agency. The information presented here is simply a snapshot of the selected systems at the point in time of the data collection process and no verification of the acquired information or testing of the systems was accomplished as part of the requirements of the statement of work associated with this Task Order.

[8] The researchers have found this to be a common problem over the years in reviewing and evaluating a variety of software systems. In general, if often seems that the promotional materials offered by some of the developers of software systems are often based on the attributes the system will eventually have as opposed to those that are currently available and manifested in actual usage. Thus, the questions associated with the matrixes were designed to identify the existing attributes in addition to those that are expected to be ultimately present, if the development of the system continues according to the indicated schedule. The researchers did not experience any attempt on the part of the developers or the end-users of the considered products to deceive in any way, shape, or form.

DESCRIPTIONS OF THE INVESTIGATED SYSTEMS

Descriptions of the following seven software systems are catalogued is this report:[9]

- ❒ Activation Information Management (AIM);
- ❒ Disaster Management Interoperability Services (DMIS);
- ❒ Infragard;
- ❒ Integrated Transportation Analysis (ITA);
- ❒ Intelligent Road and Rail Information Server (IRRIS);
- ❒ MobileShield™; and
- ❒ Surface Transportation Information Sharing and Analysis Center (ST-ISAC).

ACTIVATION INFORMATION MANAGEMENT (AIM)

The Activation Information Management (AIM) system, used most notably by the US DOT, is one part of a larger package labeled E Team.

Background

The product is an Internet-based emergency management information processing system, designed to provide users with information sharing tools related to facility and event security, disaster preparedness and recovery, and business continuity. AIM enables users to report pertinent threat information. Alerts can then be posted for other users and notification lists can be activated, thus contacting the responsible agencies and officials. It may be structured using various module configurations based on the specific requirements of an end-user. Features available in the product release that was scheduled for August 2003 include personnel management, hazard modeling, enhanced GIS mapping, *E Team to E Team Communication*, Crystal Reports[10] interfacing, real-time messaging capabilities, Information Technology threat tracking, and disaster relief organization.

Initial testing began in 1999 with the City of Los Angeles, California. The current list of customers includes:

---

[9] The developers of the considered systems and their end-users have provided the information reported here. The statement of work for the Task Order did not include requirements or resources for the verification of the information or the testing of the suggested functionality of the systems. These activities will have to be completed by each of the state DOTs with respect to the software systems considered to most closely satisfy each of their expected needs.

[10] Crystal Reports is software that enables a user to transform data reports into interactive content that can be viewed and queried. Information reporting is integrated into a variety of applications, including .NET, Java™ and COM. Reports are designed from multiple sources and enable self-service interactive viewing using the Internet. End users should be able to access and interact with reports via portals, wireless devices and Microsoft Office products. Additional information can be obtained at http://www.crystaldecisions.com/products/crystalreports/default.asp. The names of developers, manufacturers, service providers, and products are used throughout this report in the interest of accuracy. Neither the National Cooperative Highway Research Program nor the McCormick Taylor Research Team members endorse any product, manufacturer, or service provider.

- ❒ United States Department of Transportation (US DOT);
- ❒ Transportation Security Administration (TSA);
- ❒ United States Department of Health and Human Services (HHS);
- ❒ United States Environmental Protection Agency (EPA);
- ❒ statewide and regional groups;
- ❒ county governments; and
- ❒ 25 US municipalities.

AIM has been used for recent events including the disaster relief and resource management efforts following the September 11, 2001 attacks in New York City, the Space Shuttle Columbia disaster material recovery process undertaken by the EPA, and emergency planning and resource management at the Salt Lake City Winter Olympic Games.

System Information

AIM uses a Web-based interface. Users may access the system from any Internet portal. The interface requires no E Team-specific software installation on users' computers. Individuals must use an Internet browser (either Internet Explorer 5.0 or Netscape Communicator 4.6 or higher) to access their E Team server. Once the server is accessed, users are prompted for a username and a valid password. The E Team server houses user-reported information and makes this data available to other E Team users.

The information being shared on the system can be housed in a variety of ways. A simple configuration may use one E Team server with all user data being stored locally. Another configuration may incorporate multiple servers with data being stored on each. In the second configuration, the *E Team to E Team Communication* feature, once made available, is expected to enable users to access the data housed on either server. Backup configurations can include a multiple server arrangement for redundancy, or services provided by SunGard through E Team to ensure server information continuity.[11] US DOT uses multiple server redundancy, hosting the system on two servers, one located in Washington, DC, and the other located in Oklahoma City, OK. Data is replicated to both servers (mirrored) so that in the event of an interruption of service at one of the facilities, all posted data will remain available.

AIM uses incident reports to communicate events occurring throughout the participating community and to disseminate incident information to all users. AIM also uses regional status reports, called situation reports, and makes these reports either available to all users or available based on a tiered access procedure, with some information available only to certain users or organizations. The system allows for facility status monitoring, relaying

[11] SunGard Business Continuity and Internet Services reportedly partners with E Team to provide system management services for application and data center outsourcing, and also offers an Applications Service Provider (ASP) delivery model. This arrangement addresses client demand for co-location and managed hosting services. Additional information is available at http://www.sungard.com. Neither the National Cooperative Highway Research Program nor the McCormick Taylor Research Team members endorse any product, manufacturer, or service provider.

transportation-specific facility information such as delays, cancellations, and closures involving airports, rail systems, ports, and highways. AIM also provides for complete resource requests to be made (including the full approval process), allowing requested resources to be tracked through deployment, and an inventory of all assets to be maintained.

All information is geo-coded on a worldwide map with color-coded icons. This GIS functionality was described by the Crisis Management Center (CMC) staff, within US DOT, as one of the shortcomings of AIM. An enhanced version of the mapping feature is scheduled to be included in an upcoming release. Road closures are managed through the mapping function showing the locations and available resources for alternative routes. The GIS feature can also be used to plan for upcoming events and activities such as parades or nuclear shipments, allowing users to geo-code maps and input start and stop dates for events.

AIM contains an action-planning feature that allows users to define objectives, tasks and subtasks. It then assigns those tasks to individuals and tracks the tasks to completion. Upon system login, checklists are generated for users, outlining tasks to be completed. Through this feature, AIM users can be searched for by name, organization or skill set.

AIM will store reference materials that users upload to the system. AIM will also save a user-defined website link list, as well as facility location and contact information for transportation facilities. Using this method, airports or other critical infrastructure sites may be pre-programmed into the system with location information (latitude and longitude) and facility manager contact information.

The complete AIM user manual is available at http://www.rspa.dot.gov/oet/aim.pdf.

User Communication

A user in response to threat information can activate AIM notification lists. Upon activation, individuals on the notification list can be contacted through their email, pager, cell phone, or PDA. Recipients receive a URL, a login ID, and a valid password for immediate system access. AIM allows documents to be shared by AIM customers. Any changes made to a document are distributed to all recipients of the original. Document originators can keep control of the material or pass control to another user or group. Users may also use text messaging to share information with other users in real-time. Chat logs are saved to keep a record of all online real-time conversations.

Functionality

AIM, as used by CMC, is the standard E Team product coupled with five additional transportation-specific forms designed specifically for US DOT. These additional forms allow for detailed transportation-related information to be reported in a mode-specific manner by a system user. AIM is used as US DOT's primary reporting tool for collecting and disseminating information on impacts to the US transportation system because of a natural or human-caused disaster. AIM is used to record events and incidents that affect

transportation. The functions of AIM are the same as the base E Team product. Alerts can be posted to the system and notification lists can be activated, contacting the necessary transportation entities and officials. AIM's package of reports is scheduled be added to E Team's latest release (R2.1) and is scheduled to be interfaced with the upcoming release (R2.2), providing a mode-specific platform for more detailed transportation information dissemination. Aside from additional transportation-specific forms, AIM is identical to the standard E Team product and the upgraded edition performs in exactly the same manner as the standard E Team interface.

Security

AIM requires the use of TCP/IP to transfer its information. With the browser-based configuration the system sits at a level above any security precautions. Depending on their perceived security requirement, user organizations may apply any available security precautions they desire, such as secure Internet data transfer technology. CMC does not implement any extra encryption to ensure security; instead the Center uses standard Internet connections for data transfer. As a result, classified information is not shared over the Center's AIM system. The highest level of shared information disseminated over the system is *For Official Use Only* (FOUO). However, steps taken to ensure a secure TCP/IP interface using available methods could allow an organization to share secure information with system users.

Training

Based on the responses of CMC staff members, who use the system on a 24-hour-per-day/ 7-day-per-week basis, the system is relatively intuitive and does not require extensive training. No formal training was provided to CMC professionals. The system was described by a CMC staff member as user-friendly and was said to be fairly forgiving of users' mistakes. AIM was part of the TOPOFF 2 nationwide, 5-day simulation event. HHS used the action-planning feature of AIM during the exercise to assign tasks and track them to completion. CMC staff indicated that there were some issues stemming from user errors during the simulation, but that these errors were due to the fact that many of those individuals using the system during the crisis exercise had no previous experience with AIM.

E Team's Project Manager for the US DOT AIM installation pointed out that the recovery mobilizations following the attacks of September 11, 2001 revealed the system's user-friendliness. In the three weeks following the event, 1,700 users involved in the recovery process became fluent with AIM. E Team does, however, have onsite training services that are available to customers.

Pricing

Due to the absence of software on customers' computers, pricing is established on a per-user basis, rather than a per-workstation basis. The listed *quantity one* price of the system is $1,900 per year. Customers purchasing larger quantities of user seats, however, can expect to pay between $500 and $1,500 per user, per year. Specific pricing would be

negotiable based on the packages purchased. On-site training is available for $150 per trainee with a minimum of 10 trainees.

Demonstrations

Online demonstrations of AIM are available by registering for participation at www.eteam.com.

Responses from the conducted interviews are outlined in the Developer and End-User Features Matrixes.

DISASTER MANAGEMENT INTEROPERABILITY SERVICES (DMIS)

Disaster Management Interoperability Services (DMIS) is an outgrowth of the Electronic Government (or e-Gov) initiative. The e-Gov management concept was launched in February 2002, seeking to use Internet-based technology to increase the directness of communication between citizens and government.

Objectives

One aspect of the e-Gov initiative was the Disaster Management e-Gov Initiative (DME-GOV), intended to significantly enhance disaster management on an interagency and intergovernmental basis. Within DME-GOV, a goal to provide one source of disaster-related data and help was established. This grew into the website, www.disasterhelp.gov. DisasterHelp.gov, a program launched as a pilot in November 2002, was intended to give federal, state and local emergency personnel on-line access to disaster management information and tools.[12] Other DME-GOV goals are to provide interoperability among disaster management electronic tools and to provide useful, electronic tools to those parts of the disaster management community that are currently still performing disaster management functions manually.

These are the objectives of the DMIS tool suite. It is primarily a tool for agencies to share information, even arising out of different disaster management software applications. This should allow horizontal information sharing (e.g., among cities or other local government units) as well as vertical information sharing (e.g., within federal, state, and local disaster agencies).

System Functions

In general, the system has three principal functions.[13]

- ❒ Allowing an exchange of tactical information including situational awareness tools, incident reporting, addressing the requirements of secondary responders, and

[12] Source: http://www.whitehouse.gov/omb/egov/downloads/E-Gov_Initiatives.pdf.
[13] The home page for DMIS can be found at http://www.cmi-services.org.

other services to allow an organization to share information about an incident with other organizations.

- ❒ Allowing users a way to find information that is stored in governmental and non-governmental databases via access to information repositories, which provide DMIS.

- ❒ Allowing access to a consequence management digital toolkit containing products that organizations can use to fit their particular structure and needs. The objective is to include access both to available governmental and commercial tools.

In particular, DMIS has developed the following capabilities.

- ❒ A common infrastructure allows users to share information with others in a very private environment. There is also a feature that ensures that users can continue to work with a tool even if communication is lost. In addition, it automatically refreshes with new information as soon as communication can be re-established.

- ❒ An administrative function has been created for use by DMIS Operating Group Administrators. It permits system administrators to establish user accounts and define user privileges for each application.

- ❒ The Tactical Information Exchange (TIE) is one of three broad groups of DMIS applications available for responders.

    - ○ *Incident Information* describes the operating picture of an incident in digital form. This application allows the user to document the situation and send it to others to help resolve. Related pictures, maps, and files can be associated with an incident information record.

    - ○ *Specific Needs Request* (SNR) is a structured way of asking for specific help to manage an incident, including discrete resources and the desired times for delivery. SNR also allows authorized organizations to respond to a request together with logistical considerations for providing them.

- ❒ Expert Reference is expected to *eventually* provide a convenient location for consequence management references. At present, it includes the following products.

    - ○ Open Source Intelligence (OSInt), a bi-monthly collection of threat information derived from unclassified sources, using automated research tools to scan news sources from all over the world.

    - ○ Standard Equipment List (SEL) is the compilation of emergency response equipment recommended by the Interagency Board. The list provides specific items by category, though not specific products.

- ❒ The DMIS tool suite is expected to *eventually* contain a large number of automated resources. At the present time, DMIS has the following capabilities.

- Desktop Mapping includes a basic Geospatial Information System (GIS) that allows DMIS users to zoom in/out, pan, define overlays, draw objects, locate icons, and enter text labels. In addition, map data can be sent to others within one's own organization and to other organizations across the country.

- DMIS Instant Messenger (DMIS IM) allows users who are currently using DMIS to rapidly communicate with each other in a manner secure enough for sensitive (though not classified) information. Messages may be exchanged with users anywhere, including outside the user's own organization.

Cost

DMIS is owned by the federal government and is provided to users for free. The only cost element to establish functionality of the software is to provide Internet access.

Application to the Transportation Industry Directly

The software is clearly more oriented toward transportation as a component of a larger disaster management and disaster response scheme. Although components of DMIS might be useful to transportation organizations including those with a proactive approach to disaster preparedness, overall, the system is not primarily transportation-oriented. At the same time, there are resources available through the website that might be useful to those in the transportation community, though perhaps not primarily as a secure communication tool.

Instant Messaging Function

Some users from the responder community are making considerable use of the DMIS IM component. It is certainly possible that transportation industry users might find this component useful, though perhaps not as a first line of secure communication. One first responder user pointed out that on September 11, 2001, the Internet was the only available communication tool for much of the day. DMIS modules have the feature that if communication is lost with the host, the tool can still be used. Once communication is reestablished, the tool refreshes from the point at which communication was lost.

Graphics

The system's graphics capabilities are particularly impressive. It now has the capability to create overlays from Ortho images over existing maps to highlight items of particular concern to users. There was a complaint that due to the shortage of broadband capacity, some of the more sophisticated features (such as near-time video transmission) could be slow.

At present, the ability to imbed images or text from other sources into messages is limited. The ability to attach items to messages is expected to shortly be a capability.

Alerting Capabilities

DMIS has some alerting capabilities but only through the system itself. There are no provisions for alerting personnel outside the system (e.g. by phone, fax, pager or PDA). As a consequence, there is no capability for pre-arranged telephone call lists.

Training

The system is intended to be near intuitive. *Big buttons* is a term the developers coined to mean a desire to build a system that was easy for almost anyone to use. The developer is willing to provide on-site training for free, within some limits, but the end-user interviewed reported little need for this.

Installation

Installing the program was described to be as easy as loading a video game. It is expected that system updates will shortly be able to be downloaded, on-line.

Security

Though DMIS has now invoked longer, alphanumeric passwords, security precautions for items such as quick screen savers and denial of account access for too many attempted errant logons are not yet fully in place and may therefore be judged inadequate for some users.

Responses from the conducted interviews are outlined in the Developer and End-User Features Matrixes.

INFRAGARD

InfraGard has been described as a partnering opportunity for private industry and the US government. InfraGard is supported by the Federal Bureau of Investigation (FBI). It was developed to encourage the exchange of information by the government and private sector members.

InfraGard is comprised of local area chapters. This structure allows private sector members and an FBI field representative to freely exchange information regarding security-related threats to the local or national infrastructure. Local chapters hold meetings on a routine basis and create executive boards to govern and share information within the InfraGard membership. Websites and email listservs are the primary tools used to provide information on a national level.

The FBI liaison for each local chapter serves as a facilitator by:

- ❒ gathering information and distributing it to members;
- ❒ educating the public and members on infrastructure protection;

- ❒ disseminating information through the InfraGard network;
- ❒ producing valuable analytical products on information received through the InfraGard network; and
- ❒ opening the doors of communication between government and private sector members.

A major benefit of joining InfraGard is that membership is free-of-charge to anyone interested in local and national security issues. To become a member, one must successfully complete the application process, including an extensive background review conducted by the FBI.

The History of InfraGard

The National InfraGard Program began as a pilot project in 1996, when the Cleveland FBI field office asked local computer professionals to assist the FBI in determining how to better protect critical information systems in the public and private sectors. From this new partnership, the first InfraGard chapter was formed to address cyber and physical threats. InfraGard became fully operational in 1998, with the creation of the National Infrastructure Protection Center (NIPC). Now that the Department of Homeland Security (DHS) has assumed many NIPC roles, the InfraGard program has become the complete responsibility of the FBI. Figure 1 provides a historical timeline of events of InfraGard.

In conjunction with representatives from private industry, the academic community, and the public sector, the FBI further developed the InfraGard initiative to expand direct contacts with the private sector infrastructure owners and operators and to share information about cyber intrusions, exploited vulnerabilities, and infrastructure threats. The initiative, encouraging the exchange of information by government and private sector members, continued to expand through the formation of additional InfraGard chapters, within the jurisdiction of each FBI field office.

InfraGard's goal is to enable the flow of information so that owners and operators of infrastructure assets can better protect themselves and the United States government can better discharge its law enforcement and national security responsibilities. InfraGard began its journey to achieve this goal with 56 chapters. Today, there are 72 active chapters and approximately 8,000 secure members across the nation.

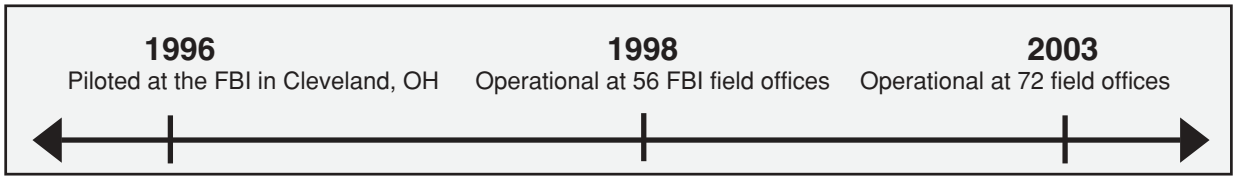


FIGURE 1: INFRAGARD TIMELINE

Application Requirements

All potential InfraGard members must complete an application process. Even if one is simply interested in becoming a non-secure member, he or she must fill out a *Non-Secure Membership Application*. Individuals interested in joining InfraGard must apply through their local chapter; however, they are given the opportunity to attend meetings as the guest of a current member before applying to become members themselves. InfraGard members are not required to attend monthly chapter meetings; however, the FBI liaison for each chapter endeavors to make each meeting a beneficial opportunity for private industry to increase the awareness of security-related issues within the local region as well as on a national level.

To become a secure member, an individual must complete and submit a Secure Membership Application. He or she must also sign and submit the following documents:

- ❒ Code of Ethics;
- ❒ National By-Laws;
- ❒ Secure Access Agreement; and
- ❒ Designated Representative Information.

These are available on the InfraGard website at http://www.infragard.net or through local FBI chapters. Unfortunately, the capability to send the required documents electronically, over the Web or through email, is not yet available. For now, they must be printed, completed, and sent via regular mail to the local FBI chapter.

All applicants for a secure membership must successfully complete a thorough background examination. The FBI is completely responsible for this sometimes-lengthy, but necessary process. The expectation for processing and approval of routine membership applications is less than 30 days. This is the result of recent improvements in the membership coordination procedure.

Incident Reporting

The InfraGard network provides many mechanisms for incident reporting. InfraGard Secure Access Members can report incidents through the secure website using the online form located in the Incident Reports section. Secure members can also report incidents by:

- ❒ contacting the Watch and Warning Unit at 202-323-3205;
- ❒ contacting the local FBI InfraGard Coordinator;
- ❒ faxing the incident report via unsecure fax to the Watch and Warning Unit at 202-323-2079 or 202-323-2082; or
- ❒ emailing the form to the Watch and Warning Unit using the secure email to infragard-hq@fbi.gov.

The FBI public website has an online incident reporting form. This form may be used by anyone wanting to report an incident to the FBI. The information is then verified and

sanitized, so it can be passed to InfraGard's secure members in the form of analytical products or threat assessments.

InfraGard Chapters

The National InfraGard Program is currently composed of 72 active chapters across the US. Chapter cities are listed in Table 1. Each listed city is hyperlinked to automatically connect the user of the electronic version of this Features Catalogue to the contact information for each chapter on the Internet. Furthermore, field offices marked with a ➡ to

TABLE 1: INFRAGARD CHAPTERS

	Albany	➡	Harrisburg		Omaha
➡	Albuquerque	➡	Honolulu		Orlando
	Anchorage	➡	Houston	➡	Philadelphia
➡	Atlanta		Indianapolis	➡	Phoenix
➡	Austin		Iowa	➡	Pittsburgh
➡	Baltimore	➡	Jackson		Portland
	Baton Rouge	➡	Jacksonville	➡	Richmond
➡	Birmingham		Kansas City		Rochester
	Boston		Knoxville		Sacramento
	Buffalo	➡	Las Vegas		Salt Lake City
➡	Charlotte		Little Rock		San Antonio
	Chattahoochee Valley	➡	Los Angeles		San Diego
	Chicago	➡	Louisville	➡	San Francisco
	Cincinnati		Madison		San Juan
➡	Cleveland		Memphis		Seattle
	Columbia	➡	Miami	➡	Springfield
➡	Columbus	➡	Milwaukee		Southern Arizona
➡	Connecticut	➡	Minneapolis	➡	St. Louis
➡	Dallas		Mobile		Tampa
	Delaware	➡	New Jersey	➡	Vermont
	Denver	➡	New Orleans	➡	Washington Field Office
➡	Detroit		New York	➡	West Virginia
➡	Eastern Carolina		Northwest Florida		
➡	El Paso	➡	Norfolk		
	Fort Wayne	➡	Oklahoma		

the left of the city name contain links to public chapter pages. These public chapter pages are used as forums to display information appropriate for the general public and non-secure members. For instance, the Philadelphia InfraGard Chapter lists an abundance of information on its website. On the first page of this site, one can view the current threat level status, a calendar of events (including chapter meetings), top headlines concerning local and national security issues, and applications for membership within InfraGard.

InfraGard Partnerships

InfraGard places its emphasis on the building of long-standing relationships among private industry leaders to foster open communication regarding security-related threats to the national infrastructure. InfraGard has formed partnerships with the following organizations, some of which can be considered governmental agencies:

- ❒ Federal Transit Administration (FTA), as a Special Interest Group;
- ❒ Small Business Administration (SBA);
- ❒ National Institute of Science and Technology (NIST);
- ❒ National Center of Manufacturing Sciences (NCMS), including about 300 manufacturers across the country; and
- ❒ Computer Security Resource Center (CSRC).

These partnerships provide a comfort level for private industry to more freely exchange critical information with the FBI through the National InfraGard Program's secure avenues.

Critical information is received from governmental agencies and the FBI relies on industry experts to determine who should receive the information. Key contacts representing each of the member groups act as a filter in determining who should receive the information. In exchange for the free software package, member groups are encouraged to provide a point of contact who will serve as an industry expert to help review, categorize, verify, and process information before it is released.

Although developing strong partnerships with industry experts is an ideal concept, InfraGard coordinators have discovered a significant setback in this process. It seems that many private industry members are not currently relaying critical information to the FBI. InfraGard's original goal was to provide an avenue for two-way communication between the private sector and the FBI. Currently, the FBI is disseminating most of the information, while many private industry users are not proactively submitting input. InfraGard has not been able to facilitate communication from the private sector. It is believed that some members may feel that sharing information with others in their particular industry may provide their competitors with an advantage in pursuing their existing customers. Still others are reluctant to share information that may allow others to conclude that they are vulnerable.

InfraGard was built on the concept of establishing trust within private industry. The system has improved relationships and encouraged the exchange of information, but it has not

fully bridged the gap between private industry and the FBI. InfraGard is a valuable asset as it exists now. Its focus, however, is different than was originally planned. Alerting private industry of security threats has been successful and communications with private industry have tremendously improved. The original goal of InfraGard assumed that private industry would respond the same way by providing critical information. There is evidence that relationships are being fostered and trust is being built. However, open communication from private industry is still very slow to develop.

Membership Offerings

Many industry businesses are becoming corporate sponsors of InfraGard by offering special services to InfraGard members. These perks are not considered endorsements by the executive board or the FBI; however, they are provided as outreach tools for some members to offer services for the purpose of supporting and educating other InfraGard members.

Most recently, McGraw-Hill Publications offered special pricing to InfraGard members on their publications via a special order form. This form has been provided to each chapter president. Furthermore, the SysAdmin, Audit, Network, Security (SANS) Institute and *TransMISsion Online (*MIS) Training Institute both offer a discount on training for all InfraGard members. MIS also offers a discount to InfraGard members for *The Forum on Information Warfare* conference scheduled for November 2003.

The Techno-Security Conference held in April each year features the Southeast InfraGard Summit as part of its agenda.[14] This event offers a discount to InfraGard members and, in 2003, offered a $100 donation to the attendees' chapter.

Federal Transit Administration (FTA)—A Special Interest Group

The Federal Transit Administration (FTA) has recently agreed to participate as a special interest group within the National InfraGard Program. FTA members can access InfraGard from a separate Web portal that provides information specific to the transportation industry. In turn, the FTA coordinator can post critical information and valuable resources on the private portal.[15] Also, security information can be forwarded to select members of FTA through separate listservs designed by the InfraGard management team, based in Baton Rouge, LA at Louisiana State University (LSU).

---

[14] Information regarding this conference can be found on http://www.techsec.com/html/Techno2003.html.
[15] The FTA liaison for InfraGard is Vicky Billet.

The FBI is willing to work with any users wishing to form a special interest group within InfraGard. Additionally, end-users can design their accounts within InfraGard to provide them with specific information related to their profession or other area of interest. Listservs are designed to send secure emails to those who request information of a specific nature.

Scope of Research

Extensive interviews of InfraGard developers were conducted on-site at LSU in Baton Rouge, LA on May 28–29, 2003. Interviewed personnel included:

- ❒ Brett Hovington, Supervisory Special Agent and InfraGard Program Manager (FBI);
- ❒ Mitzi Madere, Content Manager (LSU);
- ❒ Michael Litchfield, Content Coordinator (LSU);
- ❒ Gretchen Stein, Assistant Director (LSU); and
- ❒ Michael Wisener, Network Administrator (LSU).

Operation of the system's Help Desk function, which is a free service to InfraGard's members, was briefly observed. The Help Desk is staffed by LSU students who provide information regarding the setup and basic functions of InfraGard. Any new end-user of InfraGard must contact the Help Desk to initially install access to the Virtual Private Network (VPN) on his or her computer. The Help Desk is available to address any question or concern expressed by members. Help Desk hours have recently been expanded to accommodate both East and West Coast users. Personnel are now available from 6:00 am to 11:00 pm, Central Time.

Special Agents Jane Marazzo and John Chesson were interviewed on-site at the Philadelphia InfraGard chapter, located within the Philadelphia FBI Field Office, on June 2, 2003. Ms. Marazzo and Mr. Chesson are responsible for serving as FBI liaisons in coordinating the membership and meetings of the Philadelphia InfraGard chapter.

Additionally, the President of InfraGard's National Executive Board, Phyllis Schneck, was contacted to complete an End-User Questionnaire. Ms. Schneck stated that responses from her staff would not be available until after the PDFR version of this Features Catalogue is submitted to NCHRP. Once received, these responses will be appropriately included in the Final Report.

Responses from the conducted interviews are outlined in the Features Matrixes. Both the Developer and End-User Matrixes can be found in that subsection.

INTEGRATED TRANSPORTATION ANALYSIS (ITA)

The Integrated Transportation Analysis (ITA) system[16] began conceptual development in 1995, though actual software development did not begin until after the events of

[16] The ITA Prototype System is a combination of specifically developed software, hardware and network (including security) that has resulted in a Virtual Private Network (VPN).

September 11, 2001.[17] Unlike any of the other systems considered in this report, ITA has been created in direct response to the perceived needs of state DOTs to have access to a secure communication network that enables the sharing of transportation security concerns, alerts, intelligence and data.[18] Its development was based on a partnership between the New Mexico State Highway & Transportation Department and Sandia National Laboratories, with support from Veridian.

The ITA proof of concept prototype (version 1) was successfully demonstrated on July 3, 2002, involving seven state DOTs, the US DOT, the FBI and five New Mexico deployment sites,[19] and again on September 4, 2002. Two additional versions have been implemented.[20]

It is important to note that the ITA system continues to evolve. The initially evaluated original version is currently referred to as the currently deployed prototype. Timothy Olivas at the New Mexico State Highway and Transportation Department provided information on this version. In contrast, Sandia National Laboratories is responsible for the ultimate development of the National System, under the direction of Michael Moulton, which has yet to be completed and is not yet deployed.[21]

ITA is currently operational using the prototype version at the following locations:

- ❒ US Transportation Security Administration (TSA), Office of Maritime and Land Security, Washington, DC;
- ❒ US DOT Crisis Management Center (CMC), Washington, DC;
- ❒ Illinois DOT, Springfield, IL;
- ❒ Maryland DOT, Hanover, MD;
- ❒ Missouri DOT, Jefferson City, MO;
- ❒ Wisconsin, DOT, Madison, WI;
- ❒ New Mexico DOT (General Office and six Highway Districts);

---

[17] The following publication has been produced and apparently distributed to those agencies currently using the ITA system: New Mexico State Highway & Transportation Department Research Bureau, *Integrated Transportation Analysis Procedure Manual*, Albuquerque, NM, December 2002. This is a "Sensitive, Need-to-Know Information" document. It contains "Restricted, Need-To-Know Information." Its contents cannot be reproduced or distributed without prior permission from David Albright, Director, NMSHTD Research Bureau, 1001 Blvd., SE, Suite 103, Albuquerque, NM 87106. Very limited published information on ITA is available.

[18] The American Association of State Highway and Transportation Officials' (AASHTO) Task Force on Transportation Security identified that a secure communication infrastructure, including an effective top-down and bottom-up capability, was needed for state DOTs before, during and after the occurrence of an emergency event. ITA was directly designed to satisfy this documented need.

[19] The following reference documents the evaluation: Balog, John N. et al, *Preliminary Draft Final Report: Evaluation of the July 3, 2002 Integrated Transportation Analysis (ITA) System Demonstration*, *Op. Cit*.

[20] The researchers have only had access to the original version 1 release of the ITA system since the "ITA Prototype Software is not openly available."

[21] Contact Michael Moulton, Project Leader, Sandia National Laboratories, Department 5845, Mail Stop 0759, PO Box 5800, Albuquerque NM 87185-0759, 505-845-8106, mwmoult@sandia.gov.

- ❒ Texas DOT, Austin, TX;
- ❒ Washington State DOT, Olympia, WA;
- ❒ Florida DOT in conjunction with the Florida Technology Transfer Center, University of Florida, Gainesville, FL;
- ❒ Washington State County Road Association Board, Olympia, WA;
- ❒ Albuquerque Emergency Management Center;
- ❒ New Mexico Emergency Management Center, Santa Fe, NM;
- ❒ New Mexico State Police, Albuquerque, NM; and
- ❒ Federal Highway Administration, NM Division (Santa Fe, NM, office) and Texas Division (Austin, TX, office).

The ITA system evaluated on July 3, 2002 contained many features summarized on its primary page, including the following:

- ❒ GIS displays;
- ❒ status indicator;
- ❒ status indicator along a timeline (also referred to as the event cone);
- ❒ GIS map properties menu;
- ❒ event viewer; and
- ❒ operational plans.

It should be noted that only the four following aspects were actually tested for competency during the evaluation on July 3, 2002:

- ❒ call center;
- ❒ secure messaging, alerts, and warnings;
- ❒ secure website; and
- ❒ user data analysis/GIS interface.

Each was found to be functional within the prototype system.

ITA's secure messaging module as the event viewer stands at the heart of the current functionality of the system. Using a VPN for sending secure messages across the Internet, this part of the system is probably the most used and currently its most useful capability. It offers near real time user-to-user communication and allows forwarding of whatever information is input by any end-user. It is possible to include attachments to messages as well, such as sound (.wav files) or pictures (.jpg or other electronic, graphic files). The developers of the prototype version acknowledge that there will be significant changes to this function in the national system version that remains under development.[22] Secure, wireless communication using the ITA system has been successful.

[22] New Mexico State Highway & Transportation Department Research Bureau, *Integrated Transportation Analysis Procedure Manual*, Op. Cit., page 12.

The ITA Call Center is able to automatically receive and record telephone calls for subsequent re-transmission, if needed. This is a particularly important feature as it allows users to listen to the original message that may, at times, communicate other information (such as tone, inflection, background noises, etc.) for messages received from those reporting incidents. The system provides for a call list, for notification purposes, as calls come into the ITA Call Center. One call list is possible for safety issues and another is available for security issues. The system also provides for remotely notifying personnel by phone and for following up if a contact is unable to confirm receipt of a message.

The secure website tracks all system messages as well as shows the alert status of the country. The contents of all logged messages as well as any attachments can also be read from the secure website.

The user data analysis/GIS interface allows users to maintain a database of resources to be accessed in a crisis. An operator of the ITA system in one part of a state (or even in an adjacent state) may need to access various databases to determine the resources available in a crisis. As with all GIS systems, many layers of information are possible, allowing the user to represent items such as personnel, supplies, equipment, vehicles and others that may need to be accessed. Of course, in the case of information that can change quickly (such as volumes of supplies), to be accurate, it must be regularly kept updated. Keeping the GIS database up-to-date is the responsibility of each end-user.

The status indicator level, with its colored, concentric rings, has the capability of communicating a threat level associated with any of five different areas of concern (user, vehicle, infrastructure, social or environmental). It is located in the middle top position of the main page and designed to give a quick visual message of the alert or incident status of any received or sent message. A message associated with a bridge collapse may cause the infrastructure circle to become colored red. Some of the other areas, for example, social, are more difficult to understand. It is also unclear as to how each of the different status indicator attributes could be a different color, and how different levels of alert can be applied to different areas of concern.

ITA also possesses the capability to store user-generated operational plans that could be invoked at various alert levels for different areas of concern. This requires end users to post the operational plans they have developed, so that they will be immediately available in the event of an emergency.

A desired future attribute of the ITA system is the capability of data mining the system's messages for buried elements and information that might indicate an imminently planned attack. At this point, it is unclear how this would be accomplished.

One element that has caused user confusion has been the status timeline indicator, also called the event cone. In theory, the cone, located in the upper right hand corner of the main page, is designed to track data as it occurs and as decision-makers take actions. Events and their timing are posted as a function of the areas of concern described above. The left side of the screen illustrates pre-incident data, the intersection of the area lines

signifies the event, and the information to the right reflects post-incident information. Each vertical line on the cone refers to an event that has occurred and is documented by a message or an action.

The ITA system together with associated hardware has, to-date, been provided free-of-charge to current users and upgrades are also without cost. All current installations have been completed by having system technicians on-site at the end-users facilities. So far, the developers have absorbed the labor and travel expenses. There are currently no maintenance agreements available; however, there is a 24/7 Help Line currently available without cost. How installation, training and maintenance will be handled in the future with the National System is unknown.

The software was primarily designed to support the highway system but could also support public transportation systems and other transportation-related agencies.

ITA could be operable 24 hours per day, 7 days per week, as long as support personnel were in place to receive and send messages. The Call Center, of course, has the capability to run automatically, though, as a practical matter, some users might regard this as undesirable.

In order to remain secure, the system must be used on a stand-alone computer. A mirroring second central processing unit (CPU) is included for redundancy. The system attains full functionality when connected to other users, including the host server and the redundant servers, via a VPN facilitated by the Internet.

ITA currently has limited practical interfaces with any other systems an agency may be using. This is due to the system's secure underpinnings. For security reasons, the system cannot be part of a local area network.

Responses from the conducted interviews are outlined in the Developer and End-User Matrixes. Because ITA is currently operational in a prototype version and being further developed into an eventual national system, the matrixes include two separate lines in response to each question.

INTELLIGENT ROAD AND RAIL INFORMATION SERVER (IRRIS)

The Intelligent Road and Rail Information Server (IRRIS) was originally developed to enable rapid deployment of people, equipment, and munitions, and to improve the global deployability of US Armed Forces. IRRIS was originally designed for the Military Traffic Management Command Transportation Engineering Agency (MTMCTEA) to assist them in analyzing infrastructure readiness from Continental United States (CONUS) forts to ports in the event of a national emergency.

The system application was initially developed in the 90's because the cold war had come to a close and the US had to shut down numerous installations at forts and ports outside of the country. Many assets needed to be returned to the US, in case of a national

emergency. IRRIS was created to display and manage these routes connecting forts and ports named Power Projection Platform (PPP) routes. The application started as a visualization tool, but has since grown to include weather and traffic conditions, and other important datasets on each of the PPP routes.

Functions

According to IRRIS' developers, the system has two primary functions:

- ❒ tracking the transport of arms, ammunition, and goods; and
- ❒ aggregating traffic information through the use of real-time data to provide decision-makers with the ability to make intelligent decisions about the transportation of arms, ammunition, and goods.

This Web-based system uses information technology (IT) to allow military users to obtain detailed, timely, and relevant information about road conditions, construction, incidents, and weather that might interfere with the movement of people and goods from forts to ports through a user-friendly browser interface on the Internet. It leverages the latest advances in the IT field, such as Geographic Information Systems (GIS) and Location-Based Services (LBS) to maximize efficiency. IRRIS provides planners with a real-time tool for gathering pertinent information about specific geographical areas and roadways.

IRRIS Developer Information

GeoDecisions, a division of Gannet Fleming located in Harrisburg, PA, began development of IRRIS in the fall of 1999. GeoDecisions and MTMCTEA jointly own IRRIS. The first version of the system was deployed in 2002 at the MTMCTEA office located in Newport News, VA.

GeoDecisions has been in the IT business since 1986 and was acquired by Gannett Fleming, a multidisciplinary consulting firm with a staff of approximately 2,000 employees, in 1992. There are approximately 110 employees at GeoDecisions, and all of them perform GIS-related job functions. There are about 20 professionals dedicated solely to IRRIS.

IRRIS Components: Major Subsystems and Functionality

IRRIS uses GIS and mapping technology to provide its users with comprehensive map drawing capabilities. GeoMedia WebMap is used to display mapping data as base maps and to overlay numerous features on them. IRRIS provides a query option for users to select an area of study based on various user-defined criteria, including:

- ❒ PPP Route Map;
- ❒ Strategic Ports;
- ❒ Power Support Platforms;
- ❒ Critical Depots;
- ❒ Weather Maps;
- ❒ Fort-Port Area;
- ❒ National Guard;
- ❒ CONUS Overview Map;
- ❒ Installation Area Map; and
- ❒ Detailed Installation Map.

A useful feature of IRRIS is its capability to combine various sources of data (layers) and display all of them in an intuitive map display format. These layers may be toggled on and off by the user at his or her discretion. Many layers also have their features identified and can display attribute information for that feature through tool tips or separate information screens. Some map layers available to users include:

- ❒ Topography Map;
- ❒ Aerial Photo;
- ❒ NavTech Roads;
- ❒ Point of Interest;
- ❒ Local Road Names;
- ❒ Detailed Rail;
- ❒ Bridges;
- ❒ Weather;
- ❒ Traffic Events;
- ❒ Overhead Photo;
- ❒ Overhead Flight;
- ❒ Route Cameras;
- ❒ National Guard;
- ❒ Real-Time Information;
- ❒ Video Logs; and
- ❒ Video Exits.

The IRRIS tracking subsystem provides in-transit visibility. It allows users to:

- ❒ monitor and track the location of Department of Defense (DOD) freight traffic on a map in real-time;
- ❒ cross-reference location information with the Global Freight Management (GFM) Systems Bill of Lading (BOL) information; and
- ❒ query both the raw location and BOL data and display the results in both tabular and mapped formats.

IRRIS has the ability to provide its users with detailed turn-by-turn, address-to-address, or latitude/longitude driving directions with total drive time and mileage. It can also calculate routes to and from Army, Navy, and Air Force installations, airports, and other known points of interest. It is capable of calculating these driving directions for the fastest or shortest route based on a variety of vehicle types [e.g., E911, Hazardous Materials (HazMats), Auto, Truck], while taking into account real-time (e.g., weather, traffic patterns, incidents) factors.

Local weather information can be transmitted to the IRRIS weather subsystem through the system's own satellite receiver. Weather data is organized and displayed in real-time by a visual presentation on detailed maps. Typical weather-related information, such as where a storm currently is and where it may be heading, can be displayed. Using Meteorlogix enhanced NEXRAD radar information (a system from the National Weather Service); IRRIS has the ability to predict the general arrival time of a storm at a given site and how severe the storm will be.

Through another Web-based interface, IRRIS can provide access to real-time traffic information by allowing the user to view live route cameras, fly-throughs, video, detailed traffic incidents, construction, and event data for 89 metropolitan areas within the continental United States. Future expected capabilities include having the system provide historic and predicted travel time and traffic data. These are intended to satisfy the long-term location-based needs of the military traffic management community by providing accurate and

thorough transportability data and maximizing the use of modeling and simulation in deployment engineering.

IRRIS' Query Builder interface guides users through the process of building sophisticated database searches in order to view the textual data in a tabular format. Managers, data analysts, and report builders are empowered with on-demand access to the data in order to make better business decisions at Internet speed. IRRIS' Query Builder also enables users to display the results of their search on a map. This GIS mapping functionality allows users to view results in a variety of formats and provides a complete picture of the data without requiring users to write complex SQL (Microsoft server) statements.

Additional Capabilities

IRRIS wireless and PDA components are expected to be able to allow users to obtain information about road conditions, construction, incidents, and weather while on the road. The wireless component of IRRIS is still in the developmental stages, but one developer goal is to allow users to provide their current location to retrieve detailed information regarding road and weather conditions, receive alerts about real-time conditions ahead, and be able to view maps and driving directions when they are needed most.

Developers are currently working on a light, handheld device for access to the functionality of IRRIS. The current device is being field tested in Iraq and Kuwait, in real time, to gain access to the Internet and log onto IRRIS. There is also an alerting and notification engine available. It monitors data feeds coming into the system and alerts the necessary users of any designated information. Alerts can currently be sent by email. IRRIS developers are evaluating the option of notification via telephone where the system can read an email alert exactly as it is written. The functions of these optional modules are to provide a wireless capability and to offer access to the system in austere conditions.

Scope of Research

At the Nationwide Summit on Secure Communication Infrastructure for Transportation Industry Emergencies (Summit) held in February 2003, the secure communication systems that were mentioned by key decision-makers within the transportation industry were noted. IRRIS was one of the systems regarded as an asset to the defense industry. A review of the capabilities of IRRIS has established that it is primarily an incident/consequence management system, and not a true threat and warning system. Although IRRIS currently provides the function of emailing specific information concerning weather conditions or traffic incidents to forewarn its users of these threats to the critical infrastructure, it does not currently provide critical security-related threat information. IRRIS is mainly used to track military shipments from forts to ports (and vice versa). It is also frequently used by the military for its GIS mapping capabilities and links to specific resources. IRRIS does not, however, provide data regarding the possibility of terrorist attacks to specific locations or systems within the critical infrastructure. This information is essential to the success of a true threat and warning system as required by the transportation industry. Yet, IRRIS's GIS mapping capabilities and query functions for

critical asset location can support the functionality of an otherwise deployed threat and warning system.

IRRIS has been used to conduct tests concerning HazMat releases and the coordination of emergency management personnel during such events. Therefore, IRRIS could be used as a training device for transportation professionals to manage an incident. By causing a test event to occur within IRRIS, the military currently tracks HazMat plume direction, speed, and other pertinent information to predict threats in specific geographical areas.[23] Mobilization efforts involving the transportation industry and other emergency management personnel and agencies might be interested in the consequence management capabilities of IRRIS as an adjunct to the installation of a purposely designed threat identification and warning system.

An extensive interview of the IRRIS Senior Development Manager, Alan Beiagi, was conducted on-site at his office on May 30, 2003. Mr. Beiagi provided thorough responses to a range of developer-oriented questions regarding the functionality of IRRIS. Mr. Beiagi has been responsible for the development and various upgrades of IRRIS since its inception in 1999.

Paul Allred, MTMCTEA Chief of Highway Engineering, was interviewed on-site in Newport News, VA on June 5, 2003. Mr. Allred serves as the IRRIS Program Manager for MTMCTEA. He uses IRRIS on a daily basis for queries regarding specific military shipments. He has arranged for the system to automatically query specific items and provide him with reports on a routine basis. IRRIS was designed to fulfill this function for any end-user at his or her request.

Mr. Douglas Plummer, a Watch Analyst at US DOT's CMC, was interviewed on June 16, 2003 to acquire a non-developer perspective of the capabilities of IRRIS.

IRRIS in the Transportation Industry

The US DOT'S CMC is responsible for crisis and disaster management coordination within the transportation industry. It is a 24-hours-a-day, 7-days-a-week multimodal operation that requires real-time information to adequately resolve transportation problems. The CMC's 18 Watch Analysts have been using IRRIS since August 2002 to track weather conditions on roadways. The analysts agree that IRRIS provides easy-to-read map graphics. Traffic information is also provided for major metropolitan areas, along with links to major metro area traffic centers on the Internet. Although the system was upgraded last month to increase response time, the end-user still must have a high-speed computer to facilitate timely access to specific maps and graphics over the Web.

[23] This is not a unique capability. For example, the following software systems provide similar capabilities: Consequence Management Interoperability Services (CMI-Services) which is owned and operated by the US Marine Corps; and the Consequence Assessment Tool Set (CATS) which is owned by the Defense Threat Reduction Agency.

Although the CMC professionals do not access IRRIS very frequently, they regard the system as a user-friendly asset to their function. One user described the map graphics as outstanding. It only took a couple of days for CMC personnel to competently access and operate the system. They reported that the software has fulfilled its originally promised purpose and has satisfied their expectations. However, the Watch Analysts recommended a few upgrades to the system, including:

- ❒ creating an incident package for large scale occurrences (e.g., railroad train derailment involving HazMats);
- ❒ enhancing the live camera capability of IRRIS while increasing its security; and
- ❒ tying these capabilities into local or state police systems.

IRRIS' developers have indicated they are open to any suggestions from customers and will attempt to integrate such capabilities into future upgrades. The developers are also willing to work with new customers, in any industry, to customize IRRIS to best satisfy local needs.

Responses from the conducted interviews are included in the Developer and End-User Features Matrixes.

MOBILESHIELD™

Northrop Grumman Corporation has developed a product, designed for secure communication, called MobileShield™. While still predominantly in development, MobileShield™ offers the promise of using conventional communications devices within a secured communication network.

Background

Northrop Grumman's MobileShield™ provides a mobile broadband network for security and emergency response applications. It allows Land Mobile Radio (LMR) systems to interoperate with cellular, telephone and Internet-based systems and applications. Integration of these disparate technologies is accomplished through application of flash-OFDM (orthogonal frequency division multiplexing), a packet-switched radio access network technology that enables always-on connections to the Internet and private networks. Through this technology, Internet Protocol (IP) addresses can be assigned to users on any element of the network, including radio-based transmissions, cell phone and satellite communications networks, and LAN (local area network)-based technologies. MobileShield™ is the result of a partnership between Northrop Grumman and Flarion Technologies.

System Information

MobileShield™ was designed to interoperate at the IP layer, providing safety or law enforcement personnel with secure communication system interoperability. Using Open Systems architecture and integrating networks using existing IP standards, the architecture is applicable to users of secure IP-based wireless data applications. Figure 2 shows an

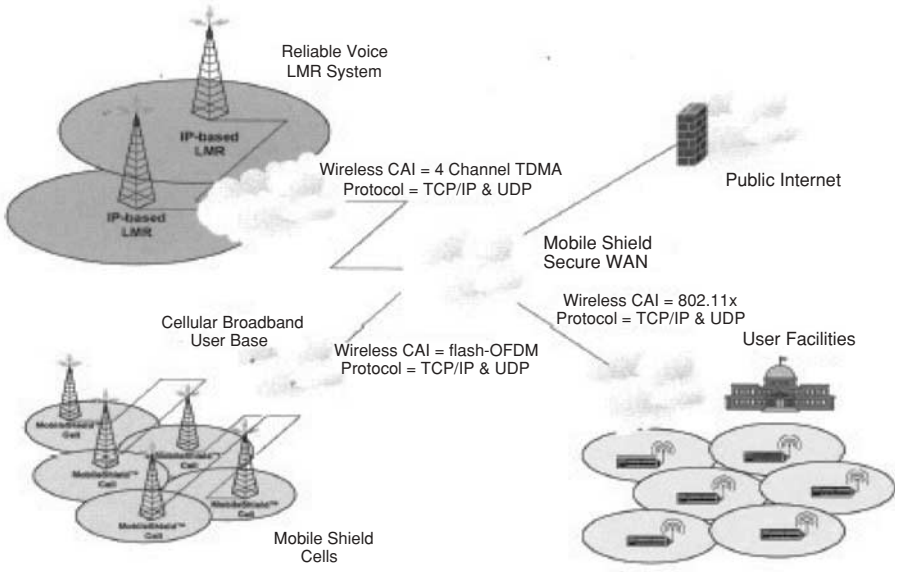


FIGURE 2: INTEGRATION OF BROADBAND CELLULAR, LAN, AND VOICE NETWORK

example of how a broadband cellular and internally deployed wireless LAN may be securely integrated with a voice network using MobileShield™.

MobileShield™ may be added to the backbone of existing infrastructure without affecting the systems already in place, such as a functioning LMR (see Figure 3). User data applications are supported on multiple Common Air Interface (CAI) mediums including existing digital LMR systems, 802.11x networks (used for wireless LAN access for buildings and short-range outdoor deployments), and 4th Generation (4G) wireless broadband technologies.

Northrop Grumman is offering 4G integration through a pilot program for demonstration purposes. Using flash-OFDM, a technology developed by Flarion, users are able to utilize a secure mobile IP access on a footprint similar to current cellular systems. In the 700 MHz spectrum band, the system can function at speeds up to 200 mph. Users may either use a PCMCIA standard card inserted into their personal system (computer, PDA, etc.) or they may use devices with the flash-OFDM chip technology integrated into the equipment.

Real-time information access affords users a data-sharing tool that can be used in various manners. One example is surveillance. The system's technology can make available secure video feeds from a camera positioned at various locations inside the system, such as an exit ramp for traffic flow monitoring or any point of heavy traffic volume. Video data can be viewed in real-time and transferred to a user's wireless device securely (see Figure 4).

A second example of real-time data transfer is the field use of criminal databases. Law enforcement personnel can use the system to receive all available information about a suspect without returning to the station. Figure 5 illustrates this example.

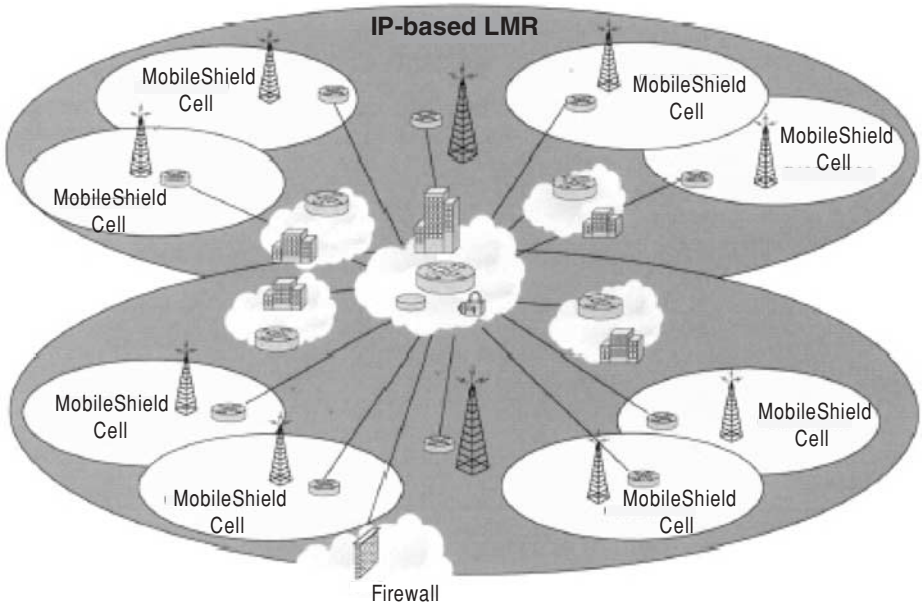


FIGURE 3: INTEGRATION OF LMR SYSTEM INTO MOBILESHIELD™

Training

Flarion's concept in developing this technology was to provide users with a method of secure wireless data transfer over an increasingly common network platform. By integrating voice data systems and transferring information using IP standards, MobileShield™ can incorporate other data transferring systems, as long as the system can have an IP address assigned to it. As a result, users are able to use systems with which

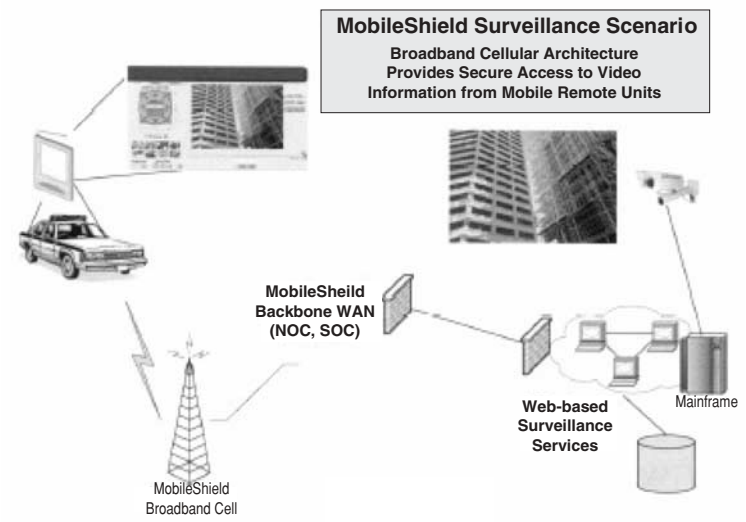


FIGURE 4: EXAMPLE SCENARIO FOR INTEGRATING RADIO-BASED COMMUNICATIONS IN WEB-BASED SURVEILLANCE SYSTEMS

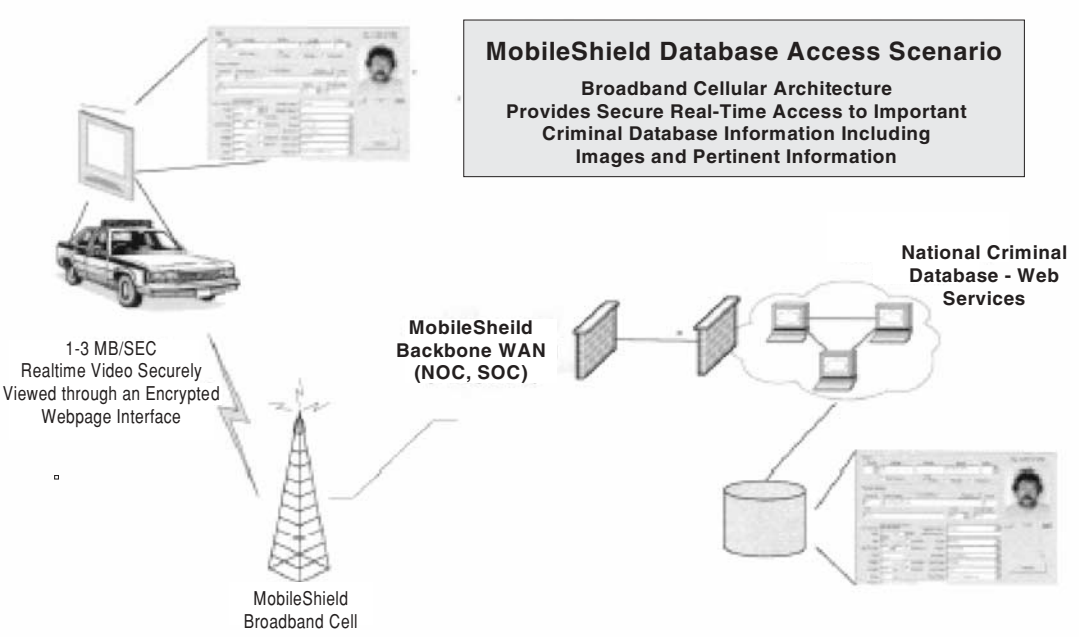


FIGURE 5: MOBILESHIELD™ DATABASE ACCESS SCENARIO

they are already familiar (laptop, cell phone, PDA) in the same manner they have always used them and training time is unnecessary. Flarion and Northrop Grumman feel that this ease of interoperability will allow existing and future technologies to be seamlessly integrated into the infrastructure.

Security

MobileShield™ is equipped with security features to protect the infrastructure. User and device authentication permits only valid network users to have access to secure information. Application layer encryption allows for continuous VPN protection of all information sent through MobileShield™. Internal alerts are generated for suspicious system, network or database activity. The system also has *denial of service* capability. It can recognize the onset of a hacking event, prevent it, and trace its origin. During testing and demonstrations of the system, Northrop Grumman has used a sophisticated software program that tries to attack the system by overwhelming it. The program is the most sophisticated disrupter known, but MobileShield™ has yet to allow legitimate users to lose service.

Pricing

Customers must purchase the equipment necessary for the system. The cost for the technology is approximately $150,000 per cell, but this price does not include the construction of the cell site. Site and tower construction will cost in the vicinity of an additional $50,000. Maintenance and modification costs are not yet determined and could be negotiated at purchase. Infrastructure equipment-related training is included in the purchase price.

Responses from the conducted interviews are outlined in the Developer and End-User Features Matrixes.

THE SURFACE TRANSPORTATION INFORMATION SHARING AND ANALYSIS CENTER (ST-ISAC)

A major interest within the transportation community has been the creation and activation of information sharing and analysis centers (ISACs) such as the Surface Transportation ISAC (ST-ISAC).

Background

ST-ISAC was originally developed, informally, for the American Association of Railroads (AAR), on request of the President of the AAR, who was designated by the US Secretary of Transportation as the *Surface Transportation Critical Infrastructure Sector Coordinator*. US DOT originally approached AAR, after the creation, in 1998, of Presidential Decision Directive 63 (PDD-63), calling for the establishment of ISACs within sectors thought critical to the national economy, such as telecommunications, banking and finance, energy, transportation, and essential government services. The original impetus of PDD-63 and of prime concern to the railroads, because of their heavy reliance on technology to conduct day-to-day operations, was cyber security. Like many of the ISACs, because it was formed out of an original concern related to cyber security, ST-ISAC is particularly well equipped to deal with cyber threats to information systems, generally, and to those of transportation organizations (and particularly the nation's railroads). As the result of a Request for Proposals (RFP) issued by the AAR, Electronic Warfare Associates Information & Infrastructure Technologies (EWA IIT) of Herndon, Virginia was selected and contracted to establish the ST-ISAC. Following the events of September 11, 2001, it was clear that additional capabilities needed to be created for physical threats as well.

The system was developed for the specific purpose of sharing cyber and physical threats related to transportation infrastructure. According to individuals interviewed at EWA IIT, much of the original cost of system development was borne by the contractor as a business decision. The system first became operational in October 2001 in an informal arrangement with Class I Railroads and AMTRAK.

The primary functions of the ST-ISAC are:

- ❒ 24/7 staffing of an information sharing and analysis center;
- ❒ connection to a network of security and intelligence analysts working in a variety of security agencies;
- ❒ secure receipt and transmission of threat information by secure email, fax, and voice; and
- ❒ a secure website for member services such as a discussion forum, sharing of best practices, plans and countermeasures to protect cyber and physical infrastructures, and other posted resources.

Reports from members, the intelligence community, law enforcement agencies, U.S. government operations centers, the Railroad Operations Center (operated by AAR) and other sources are normally analyzed by ISAC analytical staff before being sent on to members. However, certain categories of critical reports are automatically routed to members, even before all details may be known. A typical set of communication pathways is illustrated in Figure 6.

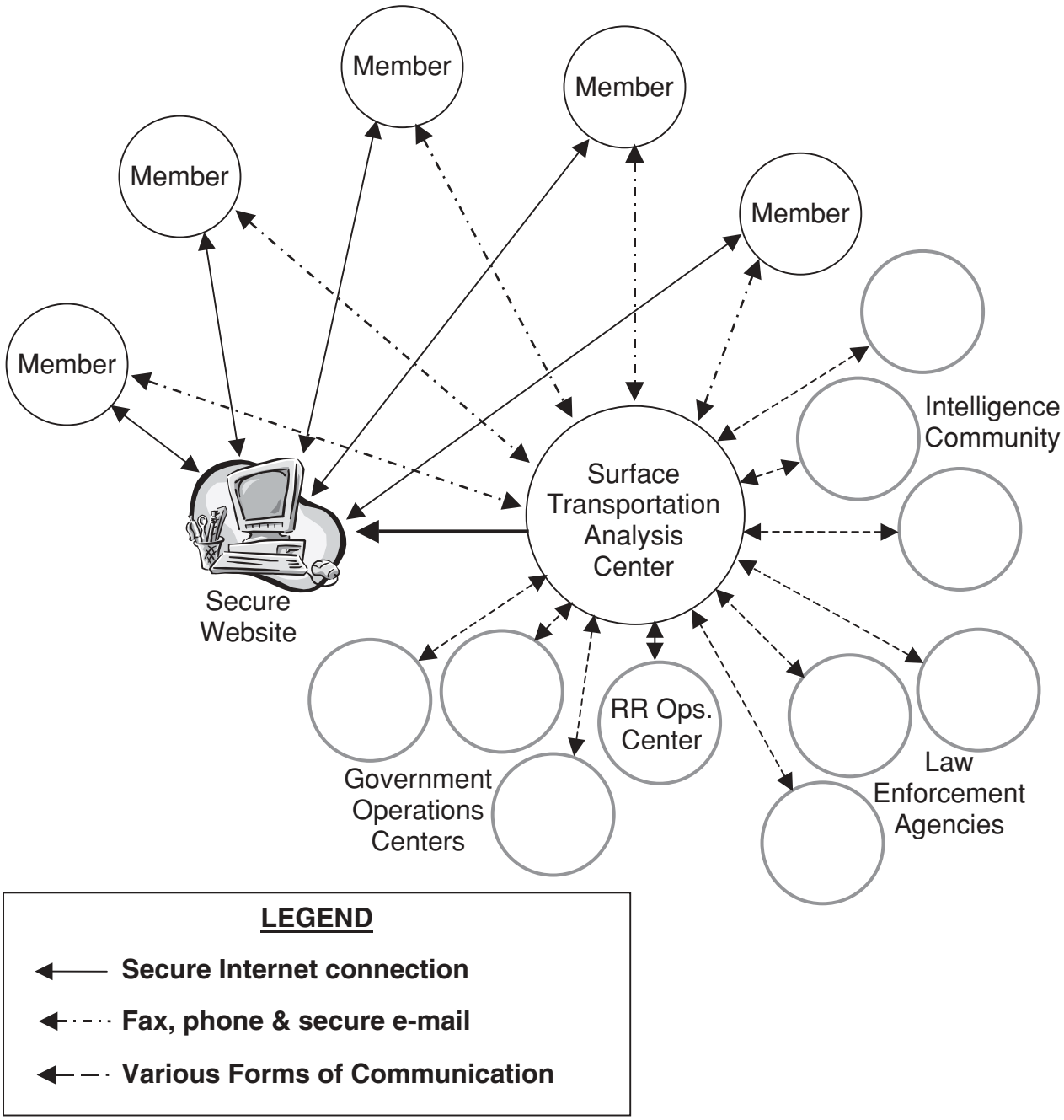


FIGURE 6: TYPICAL ST-ISAC INFORMATION PATHWAYS

In a relatively recent move, ST-ISAC now accommodates a new group of members from the public transportation industry, in addition to the original members from the Railroad industry. This has been made possible by a substantial grant from TSA via FTA, which will fund the involvement of a large number of public transportation end-users for a period of two years. The American Public Transportation Association (APTA) was designated the sector coordinator for the public transportation industry by US DOT in January 2003. The 50 largest public transportation systems in the country were added to the ST-ISAC in advance of more general participation. Additional smart cards and readers, necessary to gain access to the secure website, were recently made available and additional public transportation systems of all sizes are therefore expected to become fully functional.[24]

Though each public transportation agency must enter into its own participation agreement with EWA IIT in order to be a part of ST-ISAC, APTA's role is to coordinate and bring the sector together, working on security issues through ST-ISAC. APTA's role, already significant in the area of public transportation security, will be enhanced through this work with US DOT in defining the industry's participation as a part of the nation's overall transportation security concept.

Representatives at both EWA IIT and APTA reiterated that even those agencies that opted not to participate in ST-ISAC would be communicated with if there were clear, specific information available that directly affected them.

Public-Private Partnership

For the private railroads, which were present at the inception of ST-ISAC, privacy and anonymity have always been a major concern. Partly, this is explained by their private sector status and their fear that competitors might gain a glimpse into their operations and benefit unduly. While this may be less of an issue for public transportation entities, who are typically publicly owned and operated and less concerned about competition, ST-ISAC reports have the capability to be submitted at a variety of levels of anonymity.

For public agencies, the relationship with private companies is an important change in philosophy. ISACs are, virtually by definition, public-private partnerships and are often incorporated as limited liability corporations (LLC). They are not believed to be subject to Freedom of Information Act enquiries. This is an important issue since ST-ISAC, as a result of its considerable function, possesses and maintains a significant file of significant security information. In the hands of evildoers, this information could be effectively used against the operation of the railroad and public transportation industries.

[24] ST-ISAC considers itself a system that primarily pushes information out to its members via secure e-mail, fax and voice transmissions as well as pager notification. Any temporary inability of some participating agencies to make use of the secure website is therefore not thought by some to be very significant (conversation between Ms. Nancy Wilson, AAR Senior Assistant Vice-President, and McCormick Taylor's Mr. Peter Bromley on May 23, 2003).

Functions of the System

In the family of secure communication information systems discussed in this report, ST-ISAC is not so much remarkable for its secure communications technology, which it does employ, but rather for the analysts to which members are connected when they pick up the phone, or send a secure email. EWA IIT employs a number of analysts who are connected to DHS branches and who assist the company with making sense out of cyber and physical threat warnings.

One of the underpinnings of ST-ISAC, as far as APTA's participation was concerned, was that the required technology would not overwhelm even the smallest public transportation operators who wanted to participate. This dictated reasonably simple practices that the industry could adopt almost immediately. As it is, some small operators will have to invest in new computers or software capable of running current generation operating system technology, such as Windows 2000. On the other hand, ST-ISAC has shown itself capable of keeping the requirements simple. Messages may be sent by secure phone and fax lines for those that have them. For others, secure email has been working well. ST-ISAC discovered that Zixmail was an off-the-shelf system that uses acceptably high levels of encryption and allows even those unwilling to invest in an account (the cost is currently $50 per year) the ability to receive secure email from the system.

The only partial caveat to this is that the volume of information generated has taken some time for some first-time users to become accustomed to, especially in the public transportation community. Some likened their first exposure to the system to being spammed. The system has been receptive, however, to redesigning reports so that background information can be more easily separated from immediate, critical items. Figure 7 illustrates the public website home page.

The system's operational philosophy is that all users within a given sector get the same information (except as may be specified differently in their profile) and are treated alike. ST-ISAC's analytical staff is comprised of a network of security and intelligence analysts who investigate reports for industry relevance and accuracy. Substantial work has been undertaken with the public transportation industry to initiate ST-ISAC's security and intelligence analysts (as well as some from TSA and other security services) into the world of public transportation. This is not so much an effort to make security professionals into transportation professionals as it is to familiarize the analysts with the industries they are helping to keep secure. Perhaps more important than these classes (which have included field trips), is the effort to build strong working teams comprised of both analysts and industry professionals. There appears to be a common realization that this partnership is critical in the security relationship for the industry. This is especially true for information that either party sees which is unusual but not clearly threat-related. On the transportation side, such information can be sent on to the analysts to see if they are uncovering a more pervasive pattern. On the intelligence side, industry experts can be consulted to see if they can make sense of technical, industry-related threat information.

It is difficult to identify how long it takes for a report to be analyzed, possibly sanitized and distributed. This is dependent upon the information received. All information that is believed to be critical is communicated immediately, even if all details are not yet known.

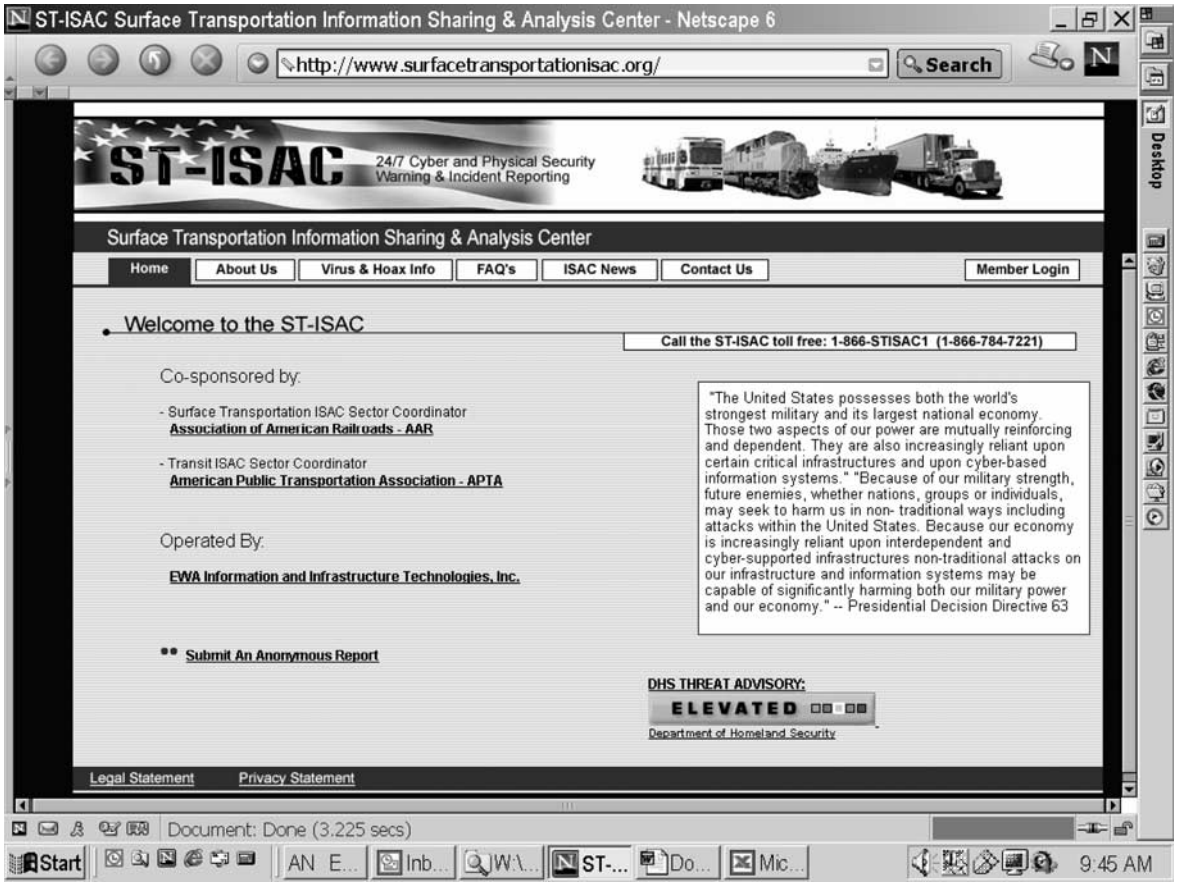


FIGURE 7: ST-ISAC PUBLIC WEBSITE HOME PAGE

ST-ISAC features full compatibility for Windows Operating Systems. ST-ISAC can also accommodate UNIX users with minor adjustments. The current configuration supports in excess of 2,000 Smart Card authenticated members and approximately 100 simultaneous, full spectrum, VPN connections.

The system appears to be so simple to use that there is no perceived need for formal training (or a manual, for that matter). Most users learned what they needed to know about the system's functions by using it. Users report virtually immediate utility with the system without training.

Though the technology is not at the center of what is being acquired when members join ST-ISAC, minor technical updates to the system are constantly being undertaken. Experimentation is being made with new modes of communication with members, in particular using PDAs.

ST-ISAC does make limited use of VPNs. Primarily, ST-ISAC does not function over VPNs. They are used mostly for communication with certain agencies and for resolution of suspected intrusions at member's systems. ST-ISAC instead uses a Smart Card authentication system that provides VPN-like security functionality. However, the Smart

Card system has improved encryption and performance over existing VPN systems. VPN solutions can, and frequently are used in conjunction with the Smart Card authentication system. Non-secure access to the private ST-ISAC website is not allowed.

ST-ISAC communicates, at this point, by means of secure phone, fax, email and pagers. Under its own philosophy, it is seen as a *push* system, meaning that it pushes information out to its members rather than requiring them to be *pulled* into accessing a secure website. There are, however, materials and resources that are too voluminous to manage any other way. These resources reside on the secure website where they can be accessed or downloaded by members with Smart Cards and readers.

ISAC Finances

The formation of ISACs as public-private partnerships is an attractive concept. However, a partnership in which a private company participates must be profitable in order to justify the enterprise. It is a point of pride for the ST-ISAC's operator that it is currently on a stable, if not profitable, basis. At the same time, all parties seem to understand that expansion of the membership base is important both to securing the future finances of ST-ISAC as well as in creating the largest possible network for collecting information on anomalous, but possibly related incidents in the broader transportation community.

At present, the cost structure is still being worked out. For a typical member, the cost is about $7,500 per year. This is acknowledged to be a potential burden to some small transportation agencies (particularly public transportation systems). While the FTA/TSA grant relieves some of these issues in the short term, a longer-term solution will be required within the two-year time frame of the current grant. The cost of membership includes 24/7 analytical (and technical) support.

Responses from the conducted interviews are outlined in the Developer and End-User Features Matrixes.

FEATURES MATRIX DESCRIPTION

The Features Matrix is a compilation of the responses to two separate sets of questions, one oriented toward developers of secure communications software products and the other toward the end-users of these products.

The developer-oriented set of questions was designed to establish, to the extent possible, the degree to which the software fulfilled certain user needs, as follows:

- ❒ ability to communicate directly with other users, virtually simultaneously;
- ❒ software (or system's) ease-of-use;
- ❒ ability to operate 24 hours per day and 7 days per week;
- ❒ limits on the number of workstations upon which the software can run;
- ❒ ability of the software to run without connection to other systems;
- ❒ timeliness with which information is transmitted;

- ability to use wireless technology to operate the system;
- standardized reports the system is capable of generating;
- ability of the system to interface with other commonly used software systems, whether in simply making use of Internet and standard office suites, in exporting data from the subject system, in importing data to the subject system or in establishing interoperability between the subject software system and other software systems;
- ability for the software to alert users of important developments by various methods, including notifying personnel away from the office;
- ability of the system to make use of GIS files; and
- security of the system, among others.

In addition, still soliciting the responses of developers, there are details of the software system important to potential users (particularly transportation industry users), but peripheral to its actual use, including:

- conceptual origin of the software;
- degree to which the software has been and continues to be revised;
- availability of the software for purchase or use by transportation agencies;
- costs to purchase; install, train, maintain, and operate the software;
- corporate stability of the company providing the software or service and its entrepreneurial interest in the future of the service or software;
- manner in which information is transmitted and to whom it is communicated directly; and
- ability of the firm that developed the software to create utility functions to produce various levels of interoperability with the end-user's existing software, among others.

Questions related to all of the subjects above are included in the Developer Questions portion of the Features Matrix. The answers received from the developers have been noted for each system considered and are also included in the Features Matrix.

In addition, another goal was to capture the opinions of end-users with the considered products. Not surprisingly, in devising applicable questions for end-users, many of the same concerns stated above prevailed, with the addition that answers to questions covering the following areas were also sought:

- organizations using the software and how the software is used;
- length of experience in using the software for both the interviewed organization and end-user, personally;
- version and configuration of the software, if applicable, the interviewed organization is using;
- perceived experience with the software's stability, reliability and user-friendliness;
- assessment of the usefulness of the software's documentation and help functions;
- adequacy of any formal training received in preparing new users for operating the software;
- experience with any developer-provided customer support in resolving problems;

- ❒ perception of whether the system or software has fulfilled its originally promised purpose;
- ❒ assessment as to whether the system or software has satisfied the end-user's original expectations;
- ❒ experience with connecting to other internal and external systems/functions;
- ❒ timeliness and quality of information received;
- ❒ perceived value of the options for and reliability of information dissemination using the system;
- ❒ assessment of the system's notification options and reliability;
- ❒ evaluation of the system's interface with other end-user programs;
- ❒ adequacy of the system's security functions;
- ❒ experience with using any available GIS capabilities;
- ❒ experience using the system to conduct test simulations or drills; and
- ❒ value delivered by any money invested in the system.

Questions related to these later subjects above are included within the End User's Questions portion in the Features Matrix. The answers received by the developers have been noted for each system considered and are also included in the Matrix.

In presenting this material, the answer to each question for each system has been grouped together, for ease of understanding and use. Using this method, each system can be quickly compared to all others for each question, while allowing full answers to be displayed. Thus, each question and the appropriate answer for each system are oriented as in the example shown in Table 2.

TABLE 2: SAMPLE FEATURES MATRIX CELL

6. When did the (software) system first become operational by an end-user?	
AIM	The software was first available August 1999.
DMIS	The software was first released on September 30, 2002.
InfraGard	The first chapter of InfraGard started in Cleveland. The National InfraGard Program began as an informal pilot program in 1996. It became operational in 1998 with the creation of NIPC. InfraGard is now completely managed by the FBI, since NIPC is being replaced by other functions of DHS.
ITA (currently deployed prototype)	Initial ITA Prototype System operational status was achieved on September 4th, 2002, with seven state DOTs, two federal sites (USDOT and FBI), and five New Mexico sites.
ITA (proposed national system)	National ITA system not yet deployed.
IRRIS	Development of IRRIS began in the fall of 1999, and the first version of the system was deployed at MTMCTEA in Newport News, VA in 2002.
MobileShield™	The system became operational in 2001.
ST-ISAC	The system first became operational in October 2001 in an informal arrangement with Class I Railroads and AMTRAK.

FEATURES MATRIXES

This subsection summarizes the responses to the interview questions posed to various system developers and end-users. The systems and services considered were:

- ❒ Activation Information Management (AIM);
- ❒ Disaster Management Interoperability Services (DMIS);
- ❒ InfraGard;
- ❒ Integrated Transportation Analysis (ITA), both the currently deployed prototype system and the national system currently under development;
- ❒ Intelligent Road/Rail Information Server (IRRIS);
- ❒ MobileShield™; and
- ❒ Surface Transportation Information Sharing and Analysis Center (ST-ISAC).

DEVELOPER FEATURES MATRIX

Table 3 is the Developer Features Matrix. It includes each of the questions asked along with the respective responses provided by the interviewee(s) representative of the software system. The presentation approach allows the reader to compare the response provided by each system representative. This should assist in the determination of which software system satisfies the greatest number of requirements established by the potential user.

Note that the responses provided were those obtained during the interviews. Verification of the information received and testing of the capabilities documented were beyond the statement of work associated with this Task Order.

In the case of the ITA software system, the developer and one existing end-user were asked to fill out the respective questionnaire matrixes directly without the use of an interviewer. The posted ITA responses are as received except when necessary to correct spelling or grammatical errors and to provide for a consistent presentation of the materials across all software systems. This approach was used for a number of reasons including: in a previous activity within the Task Order the McCormick Taylor Research Team (Team) had evaluated several competency areas associated with the ITA system and were therefore somewhat familiar with that earlier version as opposed to the current version; and the Team did not want their previous experience with the software system to influence in any way the words that were recorded during the interview and eventually posted in the Features Matrixes.

It is strongly urged that before any of these systems are acquired or purchased they should be thoroughly tested by the potential user in their then current environment or a similar environment and that functional specifications regarding the actual capabilities of the desired software system be comprehensively developed and included in the procurement bid package used by the procuring agency. The information presented here is simply a snapshot of the selected systems at the point in time of the data collection process and no verification of the acquired information or testing of the systems was accomplished as part of the requirements of the statement of work associated with this Task Order.

TABLE 3: DEVELOPER FEATURES MATRIX

1. For whom was the (software) system developed?	
AIM	E Team is a commercial off-the-shelf emergency/crisis management system. AIM is a version of the E Team system and includes several custom forms that were designed specifically for USDOT.
DMIS	Disaster Management Interoperability Services (DMIS) was developed for the responder community by the Disaster Management Program Office within the Department of Homeland Security, CIO. The original development effort pre-dated September 11, 2001.
InfraGard	InfraGard was developed for the private sector to build relationships with the owners and operators of the critical infrastructure.
ITA (currently developed prototype)	It is important to understand some basics of the ITA Prototype system. The ITA prototype was developed with State Transportation Agencies in mind, as they voiced transportation security concerns immediately following the murderous attacks on America on September 11th, 2001. The ITA Prototype provides a proof of concept for these State Transportation Agencies to share concerns securely. The proof of concept was successfully demonstrated on July 3rd, 2002 and again on September 4th, 2002. The seven participating states unanimously asked for the ITA Prototype System to remain operational to continue as their only secure means of communication. The Prototype System is not just software, but rather is a combination of specifically developed software, hardware, and network (including security). This has resulted in a Virtual Private Network (VPN) that is the ITA Prototype System.
ITA (proposed national system)	The software for the national system will be developed for the end users of the deployed system. Most of these will be for State

	Transportation Agencies, but some will be based upon national government needs.
IRRIS	IRRIS was developed for the Military Traffic Management Command Transportation Engineering Agency (MTMCTEA) to assist them in analyzing infrastructure readiness from the continental United States (CONUS) forts to ports (and vice versa) in the event of a national emergency.
MobileShield™	The focus of the development process was the homeland security, public safety, and law enforcement arenas. The product was being developed prior to 9/11 but the concept seemed to make much more sense after the tragedy.
ST-ISAC	ST-ISAC was originally developed, informally, for the American Association of Railroads (AAR), on request of the President of the AAR, who is designated by the Secretary of Transportation as the *Surface Transportation Critical Infrastructure Sector Coordinator*. Later, EWA IIT was formally contracted to establish ST-ISAC.
2. For what original purpose was the (software) system developed?	
AIM	There have been several revisions to E Team. The last AIM update was to tie it to the V1.6 product. AIM was scheduled to be updated to E Team R2 in the summer of 2003. This system will have the 5 custom AIM forms making them transportation specific. TSA currently uses E Team R2. By adding the forms into R2, USDOT and TSA can both use the product.
DMIS	The primary purpose of the software is to establish interoperability and information sharing, both horizontally (among states, counties, and municipalities) and vertically (among states and counties and municipalities). Secondly, it was designed to provide digital tools to jurisdictions that do not have digital tools.
InfraGard	The system was originally established to respond to cyber-threats. Law Enforcement Online (LEO) was also originally created for this purpose, but is only available to law enforcement officers. InfraGard is available to any individual or group approved by the FBI through an extensive background check. The success of InfraGard is dependent upon LEO because they share the same resources. LEO is currently the most stable it has ever been, in regards to funding and programming. The National Infrastructure Protection Center (NIPC), which is being partially replaced by the National Cyber Security Division (NCSD) of the Department of Homeland Security (DHS), was originally considered as a response to cyber threats, but with the creation of Presidential Decision Directive (PDD) 63 in 1998, NIPC was required to protect both cyber and physical threats to the critical infrastructure. InfraGard now follows these guidelines to communicate both types of threats.
ITA (currently	As stated in #1, the ITA Prototype System is in response to State

developed prototype)	Transportation Agencies to support a secure communication network that enables sharing of transportation security concerns, alerts, intelligence and data.
ITA (proposed national system)	The basis for some of the software envisioned to be used in the national ITA system will derive from the initial ITA prototype, and some from DOE development activities.
IRRIS	The system application was initially developed because the cold war had come to a close and the US had to shut down installations on forts and ports outside of the US. Many assets needed to be moved back inside the US, in case of a national emergency. IRRIS was originally created to display and manage these routes connecting forts and ports, called Power Projection Platform (PPP) routes. Also, during wartime, all assets need to be moved from forts to ports to be shipped out to the rest of the world. The application started as a visualization tool, but has since grown to a much larger project. The initial vision changed as the application grew. Currently, weather and traffic information, among other important data sets, are provided in addition to the PPP routes.
MobileShield™	The system was designed to provide a communications infrastructure incorporating high-speed broadband, interoperable with wireless communications, and was designed to be secure.
ST-ISAC	The system was developed for the specific purpose of sharing cyber and physical threats related to transportation infrastructure. Most of the costs of the system development were borne by Electronic Warfare Associates Information and Infrastructure Technologies (EWA IIT).
3. What are the primary functions of the (software) system?	
AIM	The system incorporates **incident reporting** to communicate what is going on at DOT regions and at DOT headquarters, disseminating any kind of emergency or transportation-related incident information, and making sure that everyone is on the same page by quickly relaying both the big picture and details. AIM includes **situation reporting**, giving the status of each region and each modal administration. Questions such as Can you do your job or Is there anything of note? are answered through this feature. A user can view the situation reports for all participating agencies. The system allows for **facility status** monitoring. These can be transportation-specific facility information such as delays, cancellations, and closures involving airports, rail systems, ports, and highways. All information is geo-coded on a worldwide **map** with color-coded icons. The shape of the icon determines the type of incident and the color describes the level of emergency.

	The system provides for **resource requests**, allowing requested resources to be tracked through deployment, and an inventory of all assets to be maintained. The feature incorporates a full approval process. The customer can choose the level of asset maintenance desired of the system. Users may set up a connection with any AIM customer, sharing any document desired. Any changes made to that document are rolled back to all recipients. Document originators can keep control of the material or pass the control to another user or group. Text messaging (chat within the application) allows for another form of real-time communication between users.
DMIS	The primary functions of the software are twofold: ❒ provide an interoperability service for the nation's responder community; and ❒ provide to responders that need them, a basic suite of digital tools.
InfraGard	The primary function of InfraGard is to share threat relevant information between the government and private industry. Currently, the FBI has been sharing information via InfraGard more frequently than have the private sectors. Monthly meetings are held to share relevant information. The larger chapters have become more active. Each chapter requires an FBI agent as a liaison and advisor. The function of the FBI agent is to provide information packets, set up speakers, facilitate or advise at meetings, and provide law enforcement expertise.
ITA (currently developed prototype)	The ITA Prototype System contains many features. Most prominent of these are: ❒ the secure messaging, alerts and warnings; ❒ the secure website; ❒ user data base for resources, messages, and intelligence; ❒ GIS interface for maps, data points, operational plans; ❒ phone call center; and ❒ Alert Status indicator and event timeline.
ITA (proposed national system)	The ITA National System will contain many of the features of the prototype system. Most prominent of these are: ❒ the secure messaging, alerts and warnings; ❒ the secure website; ❒ user data base for resources, messages, and intelligence; ❒ GIS interface for maps, data points, operational plans; ❒ phone call center; and ❒ Alert Status indicator and event timeline.

	Other features will be added as determined during the requirement gathering phases of the project.
IRRIS	IRRIS has two primary functions: ❒ track arms, ammunition, and goods; and ❒ aggregate traffic information through the use of real-time data to give decision makers a tool to make intelligent decisions about the transportation of arms, ammunition, and goods.
MobileShield™	The system provides a communications infrastructure that incorporates high-speed broadband, is interoperable with wireless communications, and is designed to use a secure IP.
ST-ISAC	The primary functions of the system are: ❒ 24/7 staffing of an information sharing and analysis center; ❒ connection to a network of security and intelligence analysts working in a variety of agencies; ❒ secure transmission of threat information by secure email, fax, voice and pager; and ❒ a secure website for member services such as a discussion forum and posted resources.
4. Are there additional modules available that increase the robustness of the (software) system?	
AIM	Specific forms and alert bulletins for the tracking of incidents have been developed for the Federal Motor Carrier Safety Administration (FMCSA) and the Federal Highway Administration (FHWA), offering specific situation reports for seven modes of transportation. The appropriate reports and forms are made available to the user depending on with what agency or organization their login is associated. Available additions to the system include enhanced GIS mapping, E Team to E Team communication, hazard modeling, a personnel management module, and enhanced report management capabilities through Crystal Reports.
DMIS	There is one suite for everyone. Users can select what parts of the suite they want to use.
InfraGard	There are about 25 modules, or computer stations, operating out of Louisiana State University (LSU). There are currently five in Washington, DC. Brett Hovington, InfraGard Program Manager and FBI Supervisory Special Agent, has a separate module of InfraGard. Every part of the system is available on the Web, but running through a VPN that only secure users, who have undergone an extensive background check, can access. The FBI

	began with 56 field offices having secure access to InfraGard. Now, they have 72 field offices equipped with the VPN.
ITA (currently developed prototype)	Additional functionalities to software will be addressed in the ITA national system. As a prototype, software upgrades were tested and issued in various versions. There have been three major releases with the latest version titled ITA 2.3.
ITA (proposed national system)	SEE # 3
IRRIS	The IRRIS application has a number of optional modules, such as wireless access to the system. Developers are currently working on an IRRIS light, handheld device. People currently in Iraq or Kuwait are testing its use in real time to gain access to the Internet and log onto IRRIS. There is also an alerting and notification engine available. It monitors data feeds coming into the system and alerts the necessary people of any information for which they wish to be notified. Alerts can currently be sent by email. IRRIS developers are looking into notification via a telephone message that reads the email alert exactly as it is written.
MobileShield™	No, there are no additional available modules.
ST-ISAC	No. All users get the same information and are treated alike.
5. What are the functions of the optional modules and what are their purchase costs?	
AIM	Enhanced GIS mapping provides users the ability to draw directly onto maps. This feature also allows for the inclusion of perimeters, plumes, text, etc. to be included on a map. The mapping enhancement is free. AIM typically has users sharing information with other users of the system by having all users log into one AIM system, but the free added feature of E Team to E Team communication enables two or more AIM systems to communicate with each other. Hazard modeling will be accessed through a consequence reduction interface. Plume models can be distributed nationwide through this module. Fees are charged for hazard modeling setup. The personnel management feature provides users with an organizational chart, allows a user to organize staffing for a 24-hour command, and can assign functional positions on a per-day/per-shift basis. The module can contain biographies and skill sets for staff members. The feature is free in the R2 version of E Team. The only price associated with the enhanced report management capabilities is the purchase price of Crystal Reports itself.
DMIS	This is not applicable to DMIS.

InfraGard	The software is provided free of charge in exchange for the sharing of threat information from private industry to the FBI. There are no additional modules at this time.
ITA (currently developed prototype)	Optional modules addressed in national ITA response.
ITA (proposed national system)	Optional modules are yet to be determined for the national ITA system.
IRRIS	Functions of the optional modules for IRRIS are to provide a wireless capability and to offer access to the system in austere conditions. The system application was developed specifically for MTMCTEA; therefore, no standard pricing exists for IRRIS or any of its additional modules. It is currently not sold to any other customers, but IRRIS developers would be open to discuss possible build-to-order options.
MobileShield™	This is not applicable to MobileShield™.
ST-ISAC	This is not applicable to ST-ISAC.
6. When did the (software) system first become operational by an end-user?	
AIM	The software was first available in August 1999.
DMIS	The software was first released on September 30, 2002.
InfraGard	The first InfraGard chapter started in Cleveland. The National InfraGard Program began as an informal pilot program in 1996. It became operational in 1998 with the creation of NIPC. InfraGard is now completely managed by the FBI, since NIPC is being replaced by other functions of DHS.
ITA (currently deployed prototype)	Initial ITA Prototype System operational status was achieved on September 4th, 2002, with seven state DOTs, two federal sites (USDOT and FBI), and five New Mexico sites.
ITA (proposed national system)	National ITA system not yet deployed.
IRRIS	Development of IRRIS began in the fall of 1999, and the first version of the system was deployed at MTMCTEA in Newport News, VA in 2002.
MobileShield™	The system became operational in 2001.
ST-ISAC	The system first became operational in October 2001 in an informal arrangement with Class I Railroads and AMTRAK.
7. How many versions of the software have been released and are operational?	
AIM	Currently, nine versions of E Team have been released (1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.6AIM, R2.0, R2.1). E Team has been involved in all major disaster situations in the United States over the past three years. Due to the amount of usage and feedback given, the software is continually improving.
DMIS	There have been two versions of the software released.

InfraGard	As a whole, the InfraGard system has been through a few different designs and upgrades. The website has been remodeled three times. Also, the VPN is upgraded about every six months, so there have been roughly five to ten upgrades since InfraGard's inception in 1998.
ITA (currently developed prototype)	The ITA Prototype System has had 3 major software releases, the latest issued in June 2003 (Version 2.3).
ITA (proposed national system)	National ITA system not yet deployed.
IRRIS	IRRIS is currently on Version 4.3. The development stages began with Version 1.0. Every six to eight weeks, a minor release is implemented, represented by the second digit on the right of the decimal point. Major releases are implemented every quarter (three to four months), represented by the first digit on the left of the decimal point.
MobileShield™	Only one version of the system has been released and is operational.
ST-ISAC	This question is not applicable to ST-ISAC.
8. What were the release dates of the various versions of the software?	
AIM	V1.2: 9/1999; V1.3: 4/2000; V1.4: 12/2000; V1.5: 4/2001; V1.6: 2/2002; R2.0: 1/2003; R2.1: 4/2003.
DMIS	The first version was released on September 30, 2002. The second version was released on June 4, 2003.
InfraGard	About every six months is an accurate estimate. When Microsoft adds something new, InfraGard is reevaluated based on approaches taken by other systems. The managers of InfraGard can contact the vendor (V1) and ask them to upgrade the system based on these approaches.
ITA (currently developed prototype)	ITA Prototype System Software Version 1 - released 3 July 2002, ITA Prototype System Software Version 2 - released 3 September 2002, and ITA Prototype System Software Version 2.3 - released 1 June 2003.
ITA (proposed national system)	National ITA system not yet deployed.
IRRIS	There have been several. The initial Version 1.0 was released in 1999, and Version 4.3 was released in April 2003. IRRIS is a constantly evolving project.
MobileShield™	The product was released in 2001.
ST-ISAC	This question is not applicable to ST-ISAC.
9. Are there additional software updates currently under development?	
AIM	AIM will be added to R2.1 and R2.2. R2.2 was scheduled for release August of 2003.

DMIS	Yes, there is a long list of future capabilities desired.
InfraGard	Yes, InfraGard as a whole is undergoing many updates and changes to the system.
ITA (currently developed prototype)	No, latest version has been tested and implemented into the ITA Prototype System operational national network. Future upgrades will be addressed in the ITA national system.
ITA (proposed national system)	National ITA system not yet deployed.
IRRIS	Yes, IRRIS developers are currently working on Versions 5.0 and 5.1 at the same time. Version 5.0 is considered a major release, while Version 5.1 involves minor changes to the system.
MobileShield™	An updated version of the software is under development.
ST-ISAC	Minor updates are constantly being undertaken. Experimentation is being made with new modes of communication with members, in particular using PDAs.
10. Describe the changes that are being made.	
AIM	E Team R2.2 AIM will incorporate 14 new ICS forms into the system, as well as personnel information, contacts, and facilities information. By including these new changes, the system will help an organization get a facility back up and running. US DOT wants to use AIM R2.2 to track IT incidents. A new module will be used to track cyber attacks. Public health forms will strengthen hospital reports to make them comply with hospital reporting requirements. R2.2AIM will be able to point to a user's GIS capabilities. The system will allow maps from outside sources to be used, providing the ability to create multiple map overlays from varying sources. A Disaster Relief module will provide donation management through new inventory asset forms; victim management for tracking transportation, food, and shelter arrangements and conditions; as well as volunteer management to coordinate deployment. All forms will be printable. The updated system will include an intelligence threat summary providing location specific threats (such as threats to bridges and tunnels) and the ability to track terrorist and gang organizations.
DMIS	In July 2003, a new version containing incident planning, target folder, and agent (e.g. biological chemical, etc.) identification is planned for release. This should allow agencies to plan response to future incidents, putting much information into the system before an incident occurs, and also assist with the identification and treatment of any suspicious substance release. In October 2003, they plan to release what they call the playbook, analogous to a football playbook for responders. This is intended

	to answer questions of appropriate situational responses to observed events. In January 2004, there is a plan to release a further interoperability capability as well as a handheld agent identification for Personal Digital Assistants (PDAs), and BACWORTH online (online access to an encyclopedia of chemical and biological information).
InfraGard	There are two new designs expected to be released in the near future within the public and secure (VPN) websites. The SSL site was scheduled to be deleted on September 1, 2003. There are currently three functional websites. These are described below. ❒ The public site, which anyone can access if they have a standard Web browser, is used as a marketing tool for the InfraGard system. It is not a secure site. ❒ The Secure Socket Layer (SSL) site, which requires a user name, password, and certification, does not require a background check. Users of this site receive limited threat data, similar to the information provided at InfraGard's public (open access) chapter meetings. The SSL site was scheduled to be deleted on September 1, 2003. ❒ The VPN site, which requires user name, password, certification, and an extensive background check, currently has approximately 8,000 members. In order to become a member of InfraGard after September 1, 2003, users must undergo complete background checks and be linked to the VPN. The public website will be updated graphically. More info on the background and executive board of InfraGard will be provided. The website will also be designed to attract new users by providing more advertising. This site will list the benefits of becoming an InfraGard member, while providing a user-friendlier interface. One major change for this site is the development of the InfraGard electronic application, which is planned to be available in the fall of 2003. General facelift design changes to the public site were scheduled to be applied in the middle of June 2003. The changes to the VPN site were planned to be applied before the end of 2003. These changes were to include an updated design and easier navigation capabilities.
ITA (currently developed prototype)	There are no changes underway for the prototype system or network. This current ITA Prototype System is operational and meets or exceeds all performance measures that were required for the proof of concept.
ITA (proposed	National ITA system not yet deployed.

national system)	
IRRIS	There is a whole list comprised of about 70 items that are currently being incorporated into the system, including both minor and major upgrades. Some examples of these upgrades are as follows. IRRIS Dynamic Alert Notification for In-Route Changes (For MTMC Operations Support). ❒ Provide alert notification and analysis tools for weather warnings/watches with the ability to reroute to safe havens, military facilities, etc. ❒ Provide ability to create a custom route (different from the existing 27 pre-defined routes) for rerouting based on notification information. ❒ Allow truckers/military operators the capability to define a custom route while taking into account weather and traffic impacts based on alerts received through IRRIS. ❒ Provide buffer distance around off-limit sites/over-limit terminals and create alert system to send notification if a tracked vehicle enters the buffer. ❒ Provide buffer distance around truck route and create alert system to send notification if a tracked vehicle exits the approved buffer area. ❒ Develop method for automated messaging if SEVs separate from tracked vehicle and approach AOR boundaries. ❒ Provide address geo-locating functionality. ❒ Add data layers to include nuclear plants, fire, police, EOD, etc. Carrier Performance Monitoring and Reporting. ❒ Build new query capability via CAT classification; trailers and Bills of Lading grouped by carrier, summarized by count; CAT or HAZMAT class trailers and/or Bill of Lading, grouped by carrier, summarized by count; trailers and/or Bill of Lading departed from installation or commercial activity, since DATE, summarized by count; trailers and/or Bill of Lading in-transit, summarized by count; arriving trailers and/or Bill of Lading at all locations, since DATE, summarized by count, grouped by CAT and HAZMAT; trailers and/or Bill of Lading currently in secure holdings, summarized by count, grouped by CAT and HAZMAT; and trailers and/or Bill of Lading currently in secure holdings that have been static since DATE, summarized by count, grouped by CAT and HAZMAT. ❒ Ongoing modifications to query and report capabilities for carrier performance monitoring.

	❒ Display location of Secure Holding Facility of last trailer location. ❒ View detailed report of Secure Holding Facility. ❒ In-Transit trailers and/or Bill of Lading impacted by weather; group by CAT, HAZMAT, summarized by count. ❒ Notify user via Email of High Visibility events. ❒ Enhance ability to generate reports on various data elements contained in IRRIS. ❒ Provide interface for users to create custom reports, summaries, and graphs/charts based on data in IRRIS. ❒ Collection of Port Infrastructure Information (1 person x 5 ports x 3 days per week). ❒ Building databases for integration of Port Studies into IRRIS (linking video-logging, executive summary, mapping, PND studies into IRRIS). ❒ Flash Presentation for Port Study capabilities. ❒ Integrate military SEV information (AORs, vehicle ids, phone numbers, etc.). In-Transit Visibility for Train and Barge Shipments. ❒ Provide up-to-date tracking information on containers and other mobile assets to include barges/ships. ❒ Work with IntelliTrans and AAR Rail Tracking to incorporate rail tracking into IRRIS. ❒ Work with Oakridge National Laboratory to incorporate CONUS routable rail into IRRIS. ❒ Ability to pick shipment by GBL, similar to Satellite Tracking. ❒ Ability to map and query the current shipment position. ❒ Ability to map and query the current track of a railcar/barge. ❒ Ability to map and query all current shipment positions. ❒ Ability to use the Query Builder to query shipment data and as an option to map it.
MobileShield™	The bandwidth is being increased to double its capacity.
ST-ISAC	Experiments are being made to the system to allow remote wireless use with PDAs. Some experimentation is also being made with the use of VPN's. A variety of VPN solutions are presently available to support special requirements.
11. When is the newest version of the software scheduled for release?	
AIM	E Team R2.1 AIM was scheduled for release in August 2003.
DMIS	The newest version was scheduled for release in July 2003.
InfraGard	The newest version was scheduled for release on September 1, 2003.

ITA (currently developed prototype)	Same as 8.
ITA (proposed national system)	National ITA system not yet deployed.
IRRIS	The newest version was scheduled for release on July 16, 2003
MobileShield™	The newest version was expected to be released in the third or fourth Quarter of 2003.
ST-ISAC	This question is not applicable to ST-ISAC.
12. Is the software openly available for purchase and use by state or municipal government agencies?	
AIM	The software is openly available for purchase and use by state or municipal government agencies.
DMIS	The software, itself, is free. The user must provide his or her own Internet connection. The software is available to state or municipal government agencies.
InfraGard	Yes, InfraGard is currently available as free software to anyone who successfully completes the application process, including a thorough background check.
ITA (currently developed prototype)	For use, not for purchase. ITA Prototype Software is not openly available.
ITA (proposed national system)	The National ITA system is not yet deployed, but expect development for most SW to be in the public domain. Other COTS SW would be available on the open market.
IRRIS	Yes, IRRIS is currently available.
MobileShield™	Yes, the product is off-the-shelf.
ST-ISAC	It is available for use. However, it is not available for purchase or ownership.
13. Please identify the names/locations of state or municipal governmental agencies currently using the system (software).	
AIM	State and regional customers include the States of Arizona, Louisiana, Utah and West Virginia; the Arizona Department of Public Safety; the Council of Governments (Washington, DC metropolitan area); and the National Governors Association (DC). Counties using the system include Clark in WA; Duchess in NY; Honolulu in HI; Lee in FL; Orange in CA; Orange in FL; Osceola in FL; and Suffolk in NY. Other users include the Sheriff's Department in San Bernardino CA, and the San Diego CA Water Authority. Municipal customers include Boca Raton, FL; Burbank, CA; Chino, CA; Culver City, CA Fire Department; Grand Terrace, CA; Honolulu, HI; Irvine, CA; Kissimmee, FL; Livermore-Pleasanton,

	CA Fire Department; Los Angeles, CA; Los Angeles, CA Business Improvement District; New York, NY; Oakland, CA; Orlando, FL; Philadelphia, PA; Phoenix, AZ; Phoenix, AZ Department of Aviation; Pico Rivera, CA; Rancho Cucamonga, CA; Rialto, CA; San Bernardino, CA Fire Department; San Francisco, CA; St. Cloud, FL; Twentynine Palms, CA; and the Washington, DC, Metropolitan Police Department.
DMIS	There are currently approximately 140 organizations using DMIS. For security reasons, the names were not released.
InfraGard	Governmental agencies currently using InfraGard are: ❒ Federal Bureau of Investigation (FBI); ❒ Federal Transit Administration (FTA), as a Special Interest Group; ❒ Small Business Administration (SBA); ❒ National Institute of Science and Technology (NIST); and ❒ National Center of Manufacturing Sciences (NCMS), including about 300 manufacturers across the country. This list is also posted on InfraGard's public website under the heading: *Partnerships*.
ITA (currently developed prototype)	The ITA prototype system (Hardware, Software, and Network) is being used by the following state departments of transportation. ❒ Transportation Security Administration - Office of Maritime and Land Security - Washington DC; Crises Management Center, USDOT, Washington DC ❒ Illinois DOT; Springfield IL ❒ Maryland DOT; Hanover, MD ❒ Missouri DOT; Jefferson City, MO ❒ Wisconsin DOT (August 2003) ❒ New Mexico DOT (7 locations; General Office and 6 Highway Districts) ❒ Texas DOT; Austin TX ❒ Washington State DOT. Olympia WA ❒ Florida DOT in conjunction with Florida Technology Transfer Center, at University of Florida. Gainesville FL ❒ Washington State County Road Association Board, Olympia WA ❒ Albuquerque Emergency Management Center ❒ New Mexico Emergency Management Center - Santa Fe NM ❒ New Mexico State Police- Albuquerque NM ❒ New Mexico National Guard- Santa Fe NM ❒ Federal Highway Administration NM Division, Santa Fe NM, office, and Texas Division, Austin TX, office

ITA (proposed national system)	National ITA system not yet deployed.
IRRIS	MTMCTEA is a federal agency, as it is part of the Department of Defense (DOD). The Naval Ammunitions Logistics Center (NALC) is also a user. No state or municipal governmental agencies are currently using the system.
MobileShield™	The product is not currently being used by state or municipal governmental agencies.
ST-ISAC	No names of state or municipal governmental members were offered due to security reasons.
14. Is the function of the system (software) appropriate for potential use by state DOTs?	
AIM	Yes, the function of AIM is appropriate for potential use by state DOTs.
DMIS	Yes. Various city and county public works agencies have been consulted with, as has FHWA.
InfraGard	Yes, the function of InfraGard is appropriate for potential use by state DOTs.
ITA (currently developed prototype)	The ITA Prototype System is being used and is appropriate for use by participating state departments of transportation.
ITA (proposed national system)	The national ITA system is not yet deployed, but its purpose is to be used by state DOTs.
IRRIS	Yes, absolutely.
MobileShield™	The function of MobileShield™ is appropriate for potential use by state DOTs.
ST-ISAC	Yes, the function of ST-ISAC is appropriate for potential use by state DOTs.
15. Is the software appropriate for potential use by bus or other transit systems?	
AIM	The system is appropriate for potential use by bus or other transit systems.
DMIS	Yes, though most applicable in their role as responders to incidents. For instance, several counties in South Carolina use the software. Public transportation is important to hurricane evacuation planning, especially for those unable to be accommodated in private vehicles. This software assists with coordination through its ability to commonly communicate with different software systems.
InfraGard	Yes, because FTA is a Special Interest Group, FTA members can access InfraGard from a separate Web portal that provides information specific to the transportation industry.
ITA (currently	Initially designed prototype is primarily highway based; however,

developed prototype)	it can be used by any transportation mode. The software could be used by bus or other transit systems.
ITA (proposed national system)	Not known at this time.
IRRIS	Yes.
MobileShield™	The system is appropriate for potential use by bus or other transit systems. It is a useful tool in video surveillance and asset tracking.
ST-ISAC	ST-ISAC currently supports many public transportation systems.
16. Please provide the names/locations of state or local transportation agencies currently using the software.	
AIM	Any of the many cities using the product and listed above could provide information pertaining to usage by local transportation agencies.
DMIS	No known transportation agencies are using the software. Some Metropolitan Planning Organizations, however, might be interested or involved.
InfraGard	FTA is the only official transportation-related entity currently using InfraGard. Police chiefs and other law enforcement officers working in the transportation environment are currently using LEO to receive threat information. InfraGard developers want to expand the software to other entities within FTA, FHWA, and other modal administrations within US DOT.
ITA (currently developed prototype)	Same as #13.
ITA (proposed national system)	National ITA system not yet deployed.
IRRIS	There are no state, local, or non-military transportation agencies other than the USDOT CMC currently using IRRIS.
MobileShield™	There are no state or local transportation agencies currently using the software.
ST-ISAC	The nation's 50 largest public transportation systems are currently using ST-ISAC, but because they do not yet have the smart cards or the readers, they are currently without access to the secure website.[25] Smart Cards/Readers were scheduled to be shipped during the week of June 2, 2003.
17. Who owns the system (software)?	
AIM	E Team, Inc. owns the software.

[25] ST-ISAC considers itself a system that primarily pushes information out to its members via e-mail, fax and voice transmissions. The temporary inability of some participating agencies to make use of the secure website is therefore not thought by some to be very significant (conversation with Nancy Wilson, AAR Senior Assistant Vice-President and McCormick Taylor's Peter Bromley on May 23, 2003).

DMIS	The United States government owns the software.
InfraGard	The FBI owns InfraGard.
ITA (currently developed prototype)	ITA Prototype System was developed by the State of New Mexico in cooperation with Sandia National Laboratories.
ITA (proposed national system)	See #12.
IRRIS	It is jointly owned by GeoDecisions, a Division of Gannett Fleming, and MTMCTEA.
MobileShield™	Flarion Technologies owns the software.
ST-ISAC	Its members own ST-ISAC. ST-ISAC is a private corporation.
18. How long has the company responsible for the system (software) been in business accomplishing this type of work?	
AIM	The company has been in business since 1998.
DMIS	This is not applicable to DMIS.
InfraGard	Since InfraGard became operational in 1998.
ITA (currently developed prototype)	This is not applicable to the ITA prototype system.
ITA (proposed national system)	This is not applicable to the national ITA system.
IRRIS	GeoDecisions has been in business since 1986. In 1992, Gannett Fleming (GF), which has been in business since 1915, purchased GeoDecisions. In recent years, GeoDecisions has operated independently, but still participates in many GF projects.
MobileShield™	The company has been in business accomplishing this type of work since 1998.
ST-ISAC	EWA IIT is about six years old. Its parent company, Electronic Warfare Associates, has been in business for 25 years.
19. How many employees work for the company responsible for the system (software) in this topic area?	
AIM	Thirty employees work in this area for the company.
DMIS	This is not applicable to DMIS.
InfraGard	About 30 FBI contracted employees work for InfraGard based in Baton Rouge, LA at the Louisiana State University (LSU). About 60 FBI agents serve as liaisons or coordinators for the nation's InfraGard chapters. Roughly 100 employees are responsible for the daily success of InfraGard.
ITA (currently developed prototype)	This is not applicable to the ITA prototype system.
ITA (proposed national system)	This is not applicable to the national ITA system.

IRRIS	There are 110 employees at GeoDecisions. All of them perform GIS-related job functions. About 20 people are dedicated solely to the IRRIS project.
MobileShield™	One hundred and fifty employees work for the company in this topic area.
ST-ISAC	EWA IIT employs about 150. The larger company, EWA, employs about 1,500 worldwide.
20. For the company responsible for the system (software), what was the gross revenue last year?	
AIM	This information was not disclosed.
DMIS	This information is not applicable to DMIS.
InfraGard	This information is not applicable to the FBI.
ITA (currently developed prototype)	This is not applicable to the ITA prototype system.
ITA (proposed national system)	This is not applicable to the national ITA system.
IRRIS	GeoDecisions' gross revenue was about $10 million last year.
MobileShield™	This information was not disclosed.
ST-ISAC	EWA IIT's gross revenue was about $30 million. The larger entity (EWA) grossed about $200 million.
21. What are the future market expectations of the company responsible for the system (software)?	
AIM	For the next couple of years the focus is on the homeland security market at the federal, state and local levels. Focus is also on corporate buyers, non-profits and utilities.
DMIS	This information is not applicable to DMIS.
InfraGard	This information is not applicable to the FBI.
ITA (currently developed prototype)	This is not applicable to the ITA prototype system.
ITA (proposed national system)	This is not applicable to the national ITA system.
IRRIS	IRRIS has many applications for different transportation agencies regarding homeland security and logistics management. GeoDecisions would like to help these agencies use IRRIS or an IRRIS-like system to satisfy their needs. There are currently some tentative goals concerning revenue, but nothing is official at this time.
MobileShield™	There are very high market expectations. The Gardner Group (telecom consultants) think that this technology will be enormous by the years 2005 to 2009. There currently is much talk about this technology around the industry. IEEE stated that this is the

	most promising area of wireless communications.
ST-ISAC	This service is acknowledged to be only very modestly profitable. Still, it is not currently losing money. There is some thought that the fact that EWA IIT is engaged in this kind of service is attractive to other clients with more profitable projects.
22. Is the software system Windows based?	
AIM	The system is Windows based.
DMIS	The software mimics Windows but is actually a Java swing client.
InfraGard	Yes.
ITA (currently developed prototype)	Yes.
ITA (proposed national system)	Though not yet deployed, it is expected to be Windows based.
IRRIS	Yes.
MobileShield™	Yes, the system is Windows based.
ST-ISAC	ST-ISAC features full compatibility for Windows Operating Systems. ST-ISAC can also accommodate UNIX users with minor adjustments.
23. If the system (software) were used by a state DOT, it would need to be operational 24 hours a day, 7 days a week. Would this cause any expected difficulties?	
AIM	There would be no difficulties with this type of arrangement. SunGard, providing protection for the system, offers a web-hosting applications service. An organization can self-host with multiple servers for redundancy or it can self-host and have SunGard back it up for them. These setups have not failed during a crisis.
DMIS	This is not a problem. The data center is manned 24 hours per day, 7 days per week.
InfraGard	The software can be used at anytime, as the VPN is already running 24/7.
ITA (currently developed prototype)	Since September 4th 2002, the ITA Prototype System has been in a 24-hour operational mode.
ITA (proposed national system)	National ITA system not yet deployed. But expect the required operational tempo to be 24/7.
IRRIS	There should be no difficulties. GeoDecisions maintains a 24/7 hosting facility. If the agency chooses, as a separate option, GeoDecisions can host a site and provide 24/7 support for it. It can also host the system at any given agency and provide any

	additional support.
MobileShield™	There is no problem with this requirement. The system was designed with this activity level in mind.
ST-ISAC	No difficulties would be expected. ST-ISAC is supported 24 hours per day, 7 days per week.
24. What is the greatest number of systemwide workstations that can simultaneously operate this software system?	
AIM	This number is only limited by the capacity of the hardware that is being used as a server.
DMIS	This number is essentially unlimited. Plans are in place to build a second data center and to provide the capability to distribute most of the server capability.
InfraGard	InfraGard is completely web-based, and therefore, unlimited.
ITA (currently developed prototype)	In the prototype mode, the secure concentrator server has been tested at up to 25 sites. Current system is operating with 23 sites.
ITA (proposed national system)	Though the national ITA system is not yet deployed, we expect the system to be flexible to allow for rapid and nonconstrained expansion as needed.
IRRIS	IRRIS is completely web-based, and therefore, unlimited.
MobileShield™	The operational limit of the system is 3 MB of data per cell site (3 mile radius). This quantity is 10 to 15 times the conventional wireless capacity.
ST-ISAC	This is limited only by bandwidth. The current configuration supports in excess of 2,000 Smart Card authenticated members and approximately 100 simultaneous, full spectrum, VPN connections.
25. Can the software be fully operational at the installation site without the need to be constantly connected to the software provider's site?	
AIM	The system can be self-hosted.
DMIS	With obvious limitations, because of its client server design, the software is designed to function quite well even if connections are lost. It is possible to continue with many functions even if the connection is lost. This is even true of communications functions that, if connections are severed, simply wait until a connection is reestablished and continue, at that time from the point of interruption. At least one agency purposely makes use of this capability by loading information on a laptop computer, severing the connection, placing the laptop on a fire truck, recording data in the field, and reestablishing the connection once back at the firehouse.
InfraGard	Yes.
ITA (currently	Most ITA prototype functionalities operate on the site hard drive

developed prototype)	and can operate in a "stand alone" configuration. Network-based functions, such as user messaging and website access, is limited under the standalone condition.
ITA (proposed national system)	Though not yet deployed, we expect the system to have some capability while not "connected" but updates and patches will most rapidly be accomplished via the interconnection.
IRRIS	Yes. IRRIS is capable of this function. This is how it is currently operating at MTMCTEA.
MobileShield™	The system can be functional without the need to be constantly connected to the software provider's site. The only requirement is T1 connectivity to the Internet. Northrop Grumman has successfully tested the system with a fed wire line, microwave, and satellite connectivity methods.
ST-ISAC	In general, the system will not operate in a meaningful way standing-alone in the user's environment. However, information and some applications can be downloaded from the ST-ISAC site and then used locally. Access to ST-ISAC provides data updates.
26. Does the software make use of a Virtual Private Network (VPN) for security purposes?	
AIM	The system does facilitate this. Use was made of a VPN for the Winter Olympics in Salt Lake City. Customers can set up their own levels of needed security. The software will work over any secure TCP/IP interface.
DMIS	Yes, the system makes use of a VPN.
InfraGard	Yes. The only way a user can access the network is through the VPN to ensure that he or she has successfully completed the application process, including an extensive background check.
ITA (currently developed prototype)	Yes, the ITA Prototype System makes use of a VPN.
ITA (proposed national system)	We envision the national ITA system to utilize VPN for security purposes. This might change if requirements dictate.
IRRIS	The Non-Secure Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET) are the non-secure and secure Military Internet backbones. SIPRNET can be considered as a VPN. IRRIS is currently running on NIPRNET, however, in August of 2003, it was scheduled to be duplicated on SIPRNET for secure access.
MobileShield™	The system makes use of a V PN for security purposes.
ST-ISAC	ST-ISAC makes use of VPNs to a limited degree. VPNs are used mostly for communication with certain agencies and for resolution of suspected intrusions at client's systems. ST-ISAC does not primarily function over VPNs. The current Smart Card

	authentication system provides VPN-like security functionality, but has improved encryption and performance over existing VPN approaches. VPN solutions can be, and frequently are, used in conjunction with the Smart Card authentication system. Non-secure access to the private ST-ISAC site is not allowed.
27. Is the system (software) able to constantly and simultaneously communicate with all other end-user agencies?	
AIM	All end-users may constantly communicate with each other.
DMIS	All end-users may constantly communicate with each other.
InfraGard	Yes.
ITA (currently developed prototype)	Yes, a central feature of the ITA Prototype System is its ability to constantly and simultaneously communicate with all other users.
ITA (proposed national system)	Though not yet deployed, we envision this to be the case.
IRRIS	Yes. IRRIS is an Internet-based system. All of its end-users are connected to a main server. Thus, the server can communicate with anyone who is connected to it.
MobileShield™	The system is able to constantly and simultaneously communicate with all other end-user agencies.
ST-ISAC	ST-ISAC has the capability through on-line discussion forums for members to communicate with one another. Still, this is not a primary system function. ST-ISAC functions, to a large degree, through user profiles. It is not expected that an identical message would normally be sent to all users, but it is possible.
28. Does the system automatically forward received, raw information to all end-user agencies?	
AIM	The raw information is made available to end-users.
DMIS	This question differentiates DMIS from some of the other products. For most end-users, DMIS software is not primarily for communication, though it can be used for that purpose. The software contains a secure instant message capability. The system is not cleared for use for classified information, just sensitive information.
InfraGard	No, information is not automatically forwarded. Operators and chapter coordinators within InfraGard determine the information that is released to the membership.
ITA (currently developed prototype)	Yes, the ITA Prototype System automatically forwards whatever information is input by the end-user.
ITA (proposed national system)	Though not yet deployed, we expect the national ITA system to have this capability/function.
IRRIS	IRRIS developers and users can feed GIS data into the main

	database of the system. Once the database is updated, all of the end-user agencies can view the most recent information.
MobileShield™	The system can automatically forward raw information to all end-user agencies.
ST-ISAC	Generally, that does not occur. Reports from members and other sources are normally analyzed through the ISAC analytical staff before being sent on to members. However, certain categories of critical reports are automatically routed to members.
29. How is the received information reviewed, categorized, verified, and otherwise processed before rendered information is distributed to system users?	
AIM	This is not applicable to the AIM system.
DMIS	This is not applicable to DMIS.
InfraGard	Critical information is received from a governmental agency and the FBI relies on industry experts to determine who should receive the information. Key contacts representing each of the member groups act as a filter in determining who should receive the information. In exchange for the free software package, member groups are encouraged to provide a point of contact who will serve as the industry expert to help review, categorize, verify, and process information before it is released. The concept is to develop strong partnerships and trust among the FBI and industry leaders.
ITA (currently developed prototype)	This is not applicable to the ITA prototype system.
ITA (proposed national system)	This is not applicable to the national ITA system.
IRRIS	The system actually performs a data analysis and checks all of the attributes to determine if the information is worthy of being sent out. IRRIS does not send out everything it receives. It verifies information through an analysis tracking system.
MobileShield™	This is not applicable to MobileShield™.
ST-ISAC	The ST-ISAC's administrator makes use of a network of security and intelligence analysts to investigate reports for industry relevance, veracity and accuracy. The administrator uses the classic intelligence cycle: 1. requirements are determined; 2. tasks are distributed to individuals to accomplish; 3. analysis takes place; 4. reports are produced and disseminated; and the process returns to the beginning.
30. How long does it take from the time information is received until a rendered	

version is disseminated to end-users?	
AIM	This is not applicable to the AIM system.
DMIS	This is not applicable to DMIS.
InfraGard	LSU is unaware of how long it takes for the information to be reviewed by the FBI, but once the information is received by LSU, it typically takes less than two hours for the information to be released to the membership. Most often, the time lapse is less than one hour from the time the information is received from the FBI. The resources are all in place. Therefore, if a message is sent, it usually goes out to InfraGard subscribers within the hour.
ITA (currently developed prototype)	This is not applicable to the ITA prototype system.
ITA (proposed national system)	This is not applicable to the national ITA system.
IRRIS	This depends on the source of data. For some information, data feeds are sent every 10 to 15 minutes. Sometimes it may take a few days for the system to analyze the data when information is received from other sources.
MobileShield™	This is not applicable to MobileShield™.
ST-ISAC	This is difficult to predict. It is dependent upon the information received. All information believed to be critical is communicated immediately, even if all details are not yet known.
31. If the system distributes raw data to end-users, how much time expires until the raw information is disseminated to end-users?	
AIM	All information is conveyed in real-time.
DMIS	The transfer of information is virtually instantaneous.
InfraGard	This is not applicable to InfraGard, as the system does not disseminate raw data.
ITA (currently developed prototype)	Information is capable of being communicated in the ITA Prototype System, from instantaneously to within minutes of having been sent.
ITA (proposed national system)	National ITA system not yet deployed. This requirement is dependent upon several factors. The time delays will be kept to a minimum.
IRRIS	This is not applicable to IRRIS, as the system does not disseminate raw data.
MobileShield™	The latency is 20-30 milliseconds. This time is insignificant and is very “real-time.”
ST-ISAC	This is not applicable to ST-ISAC, as the system does not disseminate raw data.
32. Can the system be configured so that information can be securely exchanged using wireless technology?	

AIM	The system can use wire SSL or VPN encryption. Any commercially available encryption technology may be applied to the system. AIM sits at a level above the encryption.
DMIS	Yes, information can be exchanged using wireless devices.
InfraGard	This capability is being reviewed for future use. If one can access email through his or her cell phone, then yes, wireless access is possible. However, there have been no requests for the VPN to be capable of this just yet. Wireless models are in the development stages.
ITA (currently developed prototype)	Secure, wireless communication has been successfully demonstrated with the prototype ITA system and network while maintaining network accessibility and security.
ITA (proposed national system)	National ITA system not yet deployed. Multiple secure communication paths will be incorporated as needed.
IRRIS	Yes. System security is a huge concern. IRRIS uses passwords and secure socket layers for transferring any data. Anyone with secure access to the system has undergone a background check.
MobileShield™	The system can be configured so that information can be securely exchanged using wireless technology.
ST-ISAC	This is currently being tested, but is not yet ready for normal distribution.
33. Can the system be installed and operate with full functionality and full security in vehicles that are moving?	
AIM	Mobile operability is dependent on the connection technology being used to take the AIM user online.
DMIS	It is unknown whether this has been attempted. It can be performed so long as an Internet connection is maintained. The communication is as secure as any wireless connection and still makes use of a VPN, so even intercepted transmissions may not be readily interpretable.
InfraGard	This is certainly a possibility, if the vehicle is able to access the Internet.
ITA (currently developed prototype)	The ITA prototype system is currently being tested for this capability.
ITA (proposed national system)	National ITA system not yet deployed. This has always been a goal of the ITA developers. If a need exists then there will be mobile wireless installations.
IRRIS	This is possible if the vehicles have access to the Web or some form of Telematix (in-car intelligence) or PDA device.
MobileShield™	The system can be installed and operate with full functionality and full security in vehicles that are moving.
ST-ISAC	This is currently being tested, but is not yet ready for normal

	distribution, though special provisions can be and have been made to meet this requirement for specific situations.
34. What types of standardized reports is the system capable of generating?	
AIM	AIM produces situation reports, facility damage reports, event resource requests, duty logs, map views, intelligence reports, and public information reports.
DMIS	Almost all of the functions of DMIS have associated reporting capability that gives the operator the capability to generate a text report. In particular, the following represent the primary functions of the software: ❒ Tactical Information Exchange is a situational awareness tool for managing incidents; ❒ Specific Needs Request enables one responder organization to seek assistance and track responses; ❒ Weather Forecast provides hour-by-hour weather forecasts for 48 hours, radar weather maps and a storm warning display for every ZIP code; ❒ Open Source Intelligence provides a summary of open source information by region of largely terrorist-related information; ❒ the Journal function provides a free text "log book" of an incident; ❒ Instant Messenger is a secure, instant messenger for responders; and ❒ the National Map function enables jurisdictions to bring an incident to the attention of higher authority by way of an icon on a map.
InfraGard	The operations center at LSU receives administrative reports, such as the quantity of users currently accessing the system. A data warehouse designed for specific trend analysis based on InfraGard data reports might be a future responsibility of the FBI.
ITA (currently developed prototype)	Currently, there are numerous standardized reports being used in the ITA prototype system, these include: Transportation Security Concerns (TSCs), Daily Operations Reports, Incident Reports, Transportation Security Information Reports (TSIRs), as well as numerous local agency reports that are available.
ITA (proposed national system)	Whatever is necessary to accomplish the mission.
IRRIS	There are many reports, perhaps close to 100 different types. Most of these are tracking reports (e.g., list of currently operating carriers, quantity of shipments, various locations of carriers, number of shipments bound for a specific port).
MobileShield™	The system will support end-user reports or communication methods.

ST-ISAC	ST-ISAC communicates, at this point, by means of secure phone, fax, email and pagers. Email reports for the public transportation industry are in the process of revision to separate out background information from more current threat reporting.
35. Does the software allow the user to customize received reports using standard word processing capabilities?	
AIM	AIM allows a user to edit text through a browser using standard Windows functions. It is also possible through a browser editor and a rich text editor. It could also be accomplished by using the Copy and Paste functions. The exporting functions to Crystal Reports are another way of accomplishing this.
DMIS	Not within a system software tool although system reports can be exported to other tools. The system will have reportable interoperability in that there will be the possibility to associate any file with an incident and share it with other end-users. This is technically a capability of the most recent software update but as of mid-June 2003 has not been activated. It is hoped that this can be accomplished by July 2003.
InfraGard	This is not applicable to InfraGard.
ITA (currently developed prototype)	Yes, the ITA Prototype System allows fully functioning windows and DOS based software compatibility.
ITA (proposed national system)	National ITA system not yet deployed.
IRRIS	Yes. IRRIS also allows for the exportation of report data to Excel or Microsoft Word as a text file.
MobileShield™	This is not applicable to MobileShield™.
ST-ISAC	Reports received via secure email may be cut and pasted into standard word processing documents.
36. Does the software system use the Web to transmit and receive information?	
AIM	The system uses the Web to transmit and receive information.
DMIS	Yes, the system uses the Web to transmit and receive information.
InfraGard	Yes, the system is completely Web and email based.
ITA (currently developed prototype)	Yes, the Internet is used to transmit and receive information. The ITA prototype system does use the Internet as a median for messaging, and ITA has its own secure website.
ITA (proposed national system)	National ITA system not yet deployed.
IRRIS	Yes, the system is completely Web-based.
MobileShield™	This is not applicable to MobileShield™.
ST-ISAC	That is one method of transmission, via secure email.

37. Does the software allow the computer on which it is installed to be simultaneously using the Internet for other functions?	
AIM	AIM allows for simultaneous use of the Internet. Built in to the application are links to other useful sites.
DMIS	Yes, It is possible to have DMIS running concurrently with an Internet browser in a separate window.
InfraGard	Yes, InfraGard allows for simultaneous use of the Internet while providing links to its homepage and other helpful websites for user convenience.
ITA (currently developed prototype)	ITA prototype system remains a part of the VPN.
ITA (proposed national system)	National ITA system not yet deployed, but developers envision this to not be the case due to security reasons.
IRRIS	Yes, IRRIS allows for simultaneous use of the Internet.
MobileShield™	This is not applicable to MobileShield™.
ST-ISAC	Any computer connected to the ST-ISAC secure site can also conduct separate Internet transactions without threatening ST-ISAC security.
38. Does the software allow materials copied from Internet Web Pages to be imported into its reports in real time?	
AIM	This may be accomplished by using standard Windows tools.
DMIS	No, it would be possible to send a web page snapshot and view it but not automatically enter it. It would require manually entering the data.
InfraGard	Yes, however, much of this information cannot be copied and directly emailed to users. Therefore, text is sent via email with a website link provided to the user. The purpose of this is to avoid any viruses from being sent via email. Both InfraGard and LEO have this capability, but InfraGard does not have video streaming available on its website just yet. Video streams cannot be copied into other programs.
ITA (currently developed prototype)	The ITA prototype system operates in a secure VPN environment. This capability is partially available and will be addressed in the national system.
ITA (proposed national system)	National ITA system not yet deployed, but would envision that, under certain conditions, this should be permitted.
IRRIS	Unfortunately, this cannot be done. All of the information is downloaded into the system's massive database. The software for the database is Oracle 9I.
MobileShield™	This is not applicable to MobileShield™.
ST-ISAC	Materials transmitted by secure email may be cut and pasted into other reports. Other text-based material may be inserted into secure email reports for forwarding or responding back.

39. Is the system capable of supporting interconnecting data fields so that information received via other venues can be *imported* to populate data fields in the system at the discretion of the end-user?	
AIM	Using the XML interface, ODBC, or a SQL real time interface, this can be accomplished. In fact, this has been proven in the corporate use of E Team for the management of personnel data.
DMIS	This is not possible at the current time. This is expected to be a future capability.
InfraGard	The InfraGard system does not directly interface with any other system. Information can be received, rendered, and then distributed through the system by the FBI.
ITA (currently developed prototype)	Currently, the prototype system is capable of supporting limited data mining and data warehousing. All ITA users can utilize this capability.
ITA (proposed national system)	National ITA system not yet deployed and these requirements have not been established.
IRRIS	IRRIS receives data feeds from about 15 government and commercial agencies. This information pertains to many topics, including: traffic data; weather booking information; logistics information; container information; and more.
MobileShield™	The system is capable of supporting this need.
ST-ISAC	Text-based information may be able to be cut and pasted from other venues into secure email. Any information could be directly transferred to secure email. As a matter of current practice, it does not normally happen.
40. Is the system capable of interconnecting data fields so that information within the software system can be *exported* to populate data fields within one or more other systems at the discretion of the end-user?	
AIM	Using the XML interface, ODBC, or a SQL real time interface, this can be accomplished. The E Team to E Team function will also support this requirement.
DMIS	This is not possible at the current time. This is expected to be a future capability.
InfraGard	As previously stated, the InfraGard system does not directly interface with any other system, but information can physically be copied, pasted, and emailed to other users, or even non-users. However, InfraGard members must sign a Secure Access Agreement (SAA) that prohibits them from sharing critical information with non-users.
ITA (currently developed prototype)	Same as above.
ITA (proposed	National ITA system not yet deployed and these requirements

national system)	have not been established.
IRRIS	Typical Microsoft Office copy and paste functions work well when extracting information from IRRIS. Interfaces can be designed to be compatible with other systems on different levels. IRRIS already feeds data into various Web-based systems and Microsoft report formats. Furthermore, IRRIS currently interfaces with a DOD system called the GTN (Global Transportation Network).
MobileShield™	The system is capable of supporting this need.
ST-ISAC	Text-based information may be able to be cut and pasted from secure email into other venues. There are no provisions for directly transferring information from a secure email message into another program screen or venue. All information is stored in common database formats at ST-ISAC, and could easily be manipulated for any purpose.
41. Is this system able to interoperate with other software systems so that information received via other venues will be automatically and seamlessly *imported* to populate data fields within the subject (software) system?	
AIM	This is possible and has already been implemented by other customers using the CMXML standard.
DMIS	This is not possible at the current time. This is expected to be a future capability.
InfraGard	No. For security reasons, it is critical that a system like InfraGard provide a single message from the FBI.
ITA (currently developed prototype)	The ITA prototype system does allow limited plug and play features that allow individual sites to incorporate existing technologies. This will be addressed in the ITA national system.
ITA (proposed national system)	National ITA system not yet deployed and these requirements have not been established.
IRRIS	Yes. IRRIS supports seamless data feeds from many commercial and government entities, as stated previously.
MobileShield™	The system is capable of supporting this need.
ST-ISAC	Information from certain designated sources and applications is received via a VPN connection and automatically written to a database. The data can then be applied in support of any other function/application. At this time, this takes place only at the ST-ISAC, not on user's computers.
42. Can the software developer create the utility function software that allows your software to automatically transfer data from another software?	
AIM	This utility function software can be developed.
DMIS	This is not applicable to DMIS.
InfraGard	This is certainly possible, but not highly probable because of the previously mentioned security issues. There are many variables.

	Why would this utility function software need to be developed? If a Special Interest Group, such as the FTA, expressed this need, then the FBI would address it then.
ITA (currently developed prototype)	This will be addressed in the ITA national system.
ITA (proposed national system)	National ITA system not yet deployed and these requirements have not been established.
IRRIS	This utility function software can be developed.
MobileShield™	This utility function software can be developed.
ST-ISAC	This is not applicable to ST-ISAC.
43. Has the system (software) developer ever developed such utility function software in the past?	
AIM	Utility function software has been developed whenever a customer has requested it.
DMIS	This is not applicable to DMIS.
InfraGard	Such a utility function has not been developed in the past, but it can be done.
ITA (currently developed prototype)	Sandia National Laboratories has developed this function.
ITA (proposed national system)	Are you guys kidding?
IRRIS	Yes, GeoDecisions writes the utility functions for most of the feeds going into IRRIS.
MobileShield™	Such a utility function has not been developed in the past, but it can be done.
ST-ISAC	This is not applicable to ST-ISAC.
44. What software products were made to be interoperable?	
AIM	Interconnected products include a real-time interface between E Team and Peoplesoft, an interface between E Team and ITSpatial for the Washington, DC Metropolitan Police Department, an interface between E Team and a handheld inventorying device/system used by EPA, and an interface between the CATS hazard modeling/consequence managing software and E Team.
DMIS	This is not applicable to DMIS.
InfraGard	This is not applicable to InfraGard.
ITA (currently developed prototype)	Unable to respond in this forum.
ITA (proposed national system)	Due to classified nature of information this question cannot be answered.

IRRIS	IRRIS easily integrates third party feeds into its tracking subsystem. Thus, IRRIS can provide a commercial off-the-shelf software (COTS) solution for any carrier. IRRIS currently receives feeds from: ❒ FedEx; ❒ APL; ❒ Lykes; ❒ Maersk; ❒ GTN Data Feed Integrated Booking System - Commercial Sealift Solution (IBS-CSS); ❒ Distribution Standard System (DSS); ❒ Automated Manifest System (AMS); and ❒ Continental US (CONUS) In-Transit Visibility.
MobileShield™	This is not applicable to MobileShield™.
ST-ISAC	This is not applicable to ST-ISAC.
45. Who were the clients on whose behalf software products were made to be interoperable?	
AIM	The Washington, DC Metropolitan Police Department, and the EPA were among the clients. Other clients were not disclosed.
DMIS	This is not applicable to DMIS.
InfraGard	This is not applicable to InfraGard.
ITA (currently developed prototype)	Unable to respond in this forum.
ITA (proposed national system)	Due to classified nature of information this question cannot be answered.
IRRIS	All of the entities listed in the previous response are the commercial carriers and/or products that were made to be interoperable with IRRIS.
MobileShield™	This is not applicable to MobileShield™.
ST-ISAC	This is not applicable to ST-ISAC.
46. What were the circumstances under which software products were made to be interoperable?	
AIM	Integration with Peoplesoft allowed the E Team personnel database to be updated with data from the corporate human resources system. The ITSpatial interface integrated 3D map rendering as a layer on E Team situation maps. EPA integrated its handheld inventorying device software with E Team during the Space Shuttle disaster material recovery process for cataloging every found shuttle artifact. The CATS consequence management situation allowed ground troop data to be requested by an E Team user and the CATS modeling software output was disseminated through the E Team system, displaying plume and

	tabular data on a situation map for users.
DMIS	This is not applicable to DMIS.
InfraGard	This is not applicable to InfraGard.
ITA (currently developed prototype)	Unable to respond in this forum.
ITA (proposed national system)	Due to classified nature of information this question cannot be answered.
IRRIS	IRRIS interfaces with these products to gain access to specific information concerning shipments. Tracking data is sometimes available, including: the location of a specific truck, the resources being transferred by the truck, and the booking or bill of lading information for a particular shipment. IRRIS can then aggregate the data received from different sources and provide one common view into different silos of data.
MobileShield™	This is not applicable to MobileShield™.
ST-ISAC	This is not applicable to ST-ISAC.
47. What were the functions of the software products that were made to be interoperable?	
AIM	Information from Peoplesoft supplied corporate human resources data to E Team personnel. In the case of the ITSpatial interface, integrated 3D maps were rendered as a layer on E Team situation maps. EPA integrated its handheld inventorying device software with E Team for cataloging artifacts from the Space Shuttle disaster. For CATS consequence management, the integration allowed ground troop data to be requested by an E Team user and CATS modeling software output to be disseminated through the E Team system.
DMIS	This is not applicable to DMIS.
InfraGard	This is not applicable to InfraGard.
ITA (currently developed prototype)	Unable to respond in this forum.
ITA (proposed national system)	Due to classified nature of information this question cannot be answered.
IRRIS	These interoperable software products provide real-time information to IRRIS based on data aggregated from a number of different sources.
MobileShield™	This is not applicable to MobileShield™.
ST-ISAC	This is not applicable to ST-ISAC.
48. What is an estimate of the costs associated with making the software products interoperable?	
AIM	A personnel interconnection would range from $5,000 to $20,000.

	An integration setup similar to the ITSpatial interface would have no cost. An integration of consequence modeling, similar to the CATS situation will range from $10,000 to $30,000. A situation similar to the interface designed for EPA will range between $5,000 and $10,000.
DMIS	This is not applicable to DMIS.
InfraGard	This is not applicable to InfraGard.
ITA (currently developed prototype)	Unable to respond in this forum.
ITA (proposed national system)	This is not applicable to the national ITA system.
IRRIS	This depends on the level of interconnection. It is estimated that this will take anywhere from one to three months of effort. This is a very rough order of magnitude, but anywhere from $100,000 to $300,000 can be spent on interoperability designs.
MobileShield™	This is not applicable to MobileShield™.
ST-ISAC	This is not applicable to ST-ISAC.
49. Does the (software) system include notification capabilities?	
AIM	The system includes notification capabilities.
DMIS	Yes, the system has alerting capabilities.
InfraGard	Alerts were sent via email to secure InfraGard members only to be on the look out (BOLO) for unusual activities immediately following 9/11. InfraGard can only alert users via email at this time. LEO has an automatic alert system that sends a pop-up message such as, “Please check LEO online for more information.” In the next couple of months, LEO will have the capability to send critical messages to cell phones, pagers, and other wireless modules, if the law enforcement officer did not view the pop-up message on his or her computer. These will serve as alternate modes of communication and will be coordinated directly from FBI headquarters. The test audience is every major police chief (about 20,000 members). The software will be able to determine if a user is logged onto the VPN (online) or not. If a police chief is not logged onto his or her LEO email, the system will automatically send the message to three alternate locations. As the predecessor to InfraGard, LEO has piloted many capabilities that InfraGard now possesses. If LEO is successful with these alternative methods of notification, InfraGard developers may also decide to provide these high-tech capabilities.
ITA (currently developed prototype)	Yes, the software includes notification capabilities.

ITA (proposed national system)	National ITA system not yet deployed and these requirements have not been established.
IRRIS	Yes. IRRIS currently provides alerts via email.
MobileShield™	MobileShield™ includes notification capabilities.
ST-ISAC	Yes, at present, these are by secure telephone, fax, email and pagers. In emergencies, communication can be made by conventional telephone.
50. What notification methods are used by the system to communicate with key employees when they are away from the office?	
AIM	The system can communicate by Blackberry device, telephone, pager, facsimile, and email.[26]
DMIS	At the present time, this is only possible within the system, though discussions are beginning with vendors about the possibility of telephonic alerting.
InfraGard	InfraGard uses email notifications only at this time.
ITA (currently developed prototype)	For the ITA prototype system: ❒ Blackberry? Yes. ❒ Telephone? Yes. ❒ Pager? Yes. ❒ Fax? Yes. ❒ Email? No.
ITA (proposed national system)	National ITA system not yet deployed and these requirements have not been established.
IRRIS	IRRIS uses email, Windows messaging or pop-ups, and can also provide text speech through a telephone or pager.
MobileShield™	The system can communicate by Blackberry device, telephone, pager, facsimile, and email.
ST-ISAC	At present, these would be limited to secure emails for remote pick-up, calls to cellular phones, or pagers.
51. Does the (software) system have the ability for users to create an unlimited number of *call lists* so that emergency notification is automatically forwarded to the appropriate people?	
AIM	The system facilitates the creation of unlimited call lists.
DMIS	This would be a future capability of telephonic alerting.
InfraGard	No, but it is possible to create more listservs (specific email lists). This has not been considered at the current time.
ITA (currently developed prototype)	In the ITA prototype system, one call list is available for safety issues and another is available for security issues.
ITA (proposed	National ITA system not yet deployed and these requirements

[26] Reference is made to a family of communication devices commonly referred to as Blackberrys. Neither the National Cooperative Highway Research Program nor the McCormick Taylor Research Team endorses or supports the use of any product or manufacturer.

national system)	have not been established.
IRRIS	This is not a primary function of IRRIS because it is not meant to be a communication system. Users can register on the IRRIS website that they would like to be alerted via email or phone about specific events or information feeds. An unlimited number of people can register themselves to be notified at any time.
MobileShield™	The software has the ability for users to create an unlimited number of call lists so that emergency notification is automatically forwarded to appropriate people.
ST-ISAC	There is no provision for different, user-defined call lists depending on circumstance. Users can define limited call lists. Normally, ST-ISAC attempts to integrate with member incident escalation procedures.
52. Does the (software) system have the ability for users to create an unlimited number of *contacts* within each call list?	
AIM	The system facilitates storage of unlimited contacts within each call list.
DMIS	This might be a future capability of telephonic alerting.
InfraGard	This is not applicable to InfraGard at the current time.
ITA (currently developed prototype)	The ITA prototype system does not limit the number of contacts.
ITA (proposed national system)	National ITA system not yet deployed and these requirements have not been established.
IRRIS	IRRIS does not have this capability at this time.
MobileShield™	The software has the ability for users to create an unlimited number of contacts within each call list.
ST-ISAC	Notification lists for fax or email could be made to be any length, though there is a practical limit. Voice notification is also limited, as a practical matter, to one or two individuals.
53. Does the system generate a notification log file indicating the date and time of the message for each person forwarded a message?	
AIM	AIM stores all notification message information.
DMIS	Yes, each item posted is logged.
InfraGard	If a message is sent via a listserv, then the message is archived. There is not a specific notification log available, but individual messages can be reviewed to determine when and to whom a message was sent. There are no log reports specifically generated for InfraGard.
ITA (currently developed prototype)	Yes, the ITA prototype system does generate log files.
ITA (proposed	National ITA system not yet deployed and these requirements

national system)	have not been established.
IRRIS	Yes. This information is kept on file and logged.
MobileShield™	The system generates a notification log file indicating the date and time of the message for each person forwarded a message.
ST-ISAC	The system generates a notification log file indicating the date and time of the message for each person forwarded a message.
54. Does the system document the date and time a notified person responded to the message?	
AIM	It is very simple to do this for email responses; however, doing this for calls made to cell phones would require the use of a dialogic callout system allowing users to initiate a dialogic call. After the call, the callout system would send AIM the callout result log that includes the time of the response.
DMIS	There is no formal way to accomplish this at the present time.
InfraGard	Yes. Please review the response to the previous question.
ITA (currently developed prototype)	Yes, the ITA prototype system documents responses.
ITA (proposed national system)	National ITA system not yet deployed and these requirements have not been established.
IRRIS	Users do not have the ability to reply or send correspondence through IRRIS. However, dates and times of all data feeds are logged for all events. Every query made by an IRRIS user is logged, but not necessarily monitored.
MobileShield™	The system documents the date and time a notified person responded to the message.
ST-ISAC	Yes, secure email can be set to return a message when people pick up their mail.
55. If no confirmation is received from a recipient, can the system automatically notify or suggest the back-up recipient, based on a pre-determined priority list?	
AIM	AIM automatically sends the message out to the whole call list.
DMIS	There is no formal way to accomplish this at the present time.
InfraGard	This capability is only available through LEO and is still in its testing phase. InfraGard currently has no plans to provide this capability.
ITA (currently developed prototype)	Yes.
ITA (proposed national system)	National ITA system not yet deployed and these requirements have not been established.
IRRIS	IRRIS does not have this capability at this time.
MobileShield™	The system can automatically notify or suggest the back-up

	recipient, based on a pre-determined priority list.
ST-ISAC	There is no current provision for this.
56. Does the system possess GIS capabilities?	
AIM	The system possesses GIS capabilities. Fully integrated ArcIMS is available at no additional cost.
DMIS	Yes, the system possesses GIS capabilities.
InfraGard	No, the system provides email notification only.
ITA (currently developed prototype)	Yes, the ITA prototype system has multiple GIS capabilities.
ITA (proposed national system)	Yes, the system has a GIS capability.
IRRIS	IRRIS is a GIS-based system.
MobileShield™	The system possesses GIS capabilities.
ST-ISAC	Analysts use a GIS-based database/application as an analytical tool at ST-ISAC. This application is keyed to "critical" member assets. This is not related, however, to resources available to members directly at their location(s).
57. Does the system accept/export standard GIS files according to standard protocols?	
AIM	Standard protocols are used for accepting and exporting GIS files.
DMIS	Yes, this is a feature of the newest version, just released.
InfraGard	This is not applicable to InfraGard.
ITA (currently developed prototype)	Yes.
ITA (proposed national system)	National ITA system not yet deployed and these requirements have not been established.
IRRIS	IRRIS currently does not accept/export standard GIS files according to standard protocols, but this could easily be accomplished.
MobileShield™	The system accepts/exports standard GIS files according to standard protocols.
ST-ISAC	This is not applicable to ST-ISAC.
58. Can the system be used to conduct test simulations and drills?	
AIM	The system can be used to conduct test simulations and drills. AIM comes with both operational and training databases. Using the training side and distribution function, users may stage a full training exercise.
DMIS	Yes, there is a box to check for *exercise*.
InfraGard	No.

ITA (currently developed prototype)	Yes.
ITA (proposed national system)	National ITA system not yet deployed and these requirements have not been established.
IRRIS	Yes. IRRIS has already been used on a number of occasions to conduct test simulations and drills.
MobileShield™	The system can be used to conduct test simulations and drills.
ST-ISAC	No, but it can support them. This has not yet been attempted by the public transportation industry.
59. What is the yearly license cost to utilize the (software) system?	
AIM	If the system is self-hosted, there is no yearly fee. The price per seat is $1,900 if only one workstation is used. When purchased in larger quantities, customers can expect a price somewhere between $500 and $1,500 per year, per user.
DMIS	There is no such yearly license cost.
InfraGard	The software is provided free of charge to users who have successfully completed a thorough background check in exchange for sharing threat information from private industry to the FBI.
ITA (currently developed prototype)	There is no annual cost to use the ITA prototype system.
ITA (proposed national system)	Not known at this time.
IRRIS	This particular version of IRRIS was built as a custom application for MTMCTEA. The cost would depend on the exact use of the system.
MobileShield™	Purchasers buy the equipment. The cost is approximately $150,000 per cell, not including the construction of the cell site that approximately costs an additional $50,000.
ST-ISAC	The cost structure is still being worked out. For a typical member, the cost is currently about $7,500 per year.
60. What is the cost to install the software per local area network?	
AIM	The system is paid for on a per user basis and requires only the usage of an internet browser.
DMIS	The process is very simple and can be performed by virtually any user. Therefore, no cost is associated with installation.
InfraGard	Installation assistance is provided over the telephone through the InfraGard Help Desk free of charge to users who have successfully completed a thorough background check in exchange for sharing threat information from private industry to the FBI.

ITA (currently developed prototype)	The ITA prototype system uses LAN/WAN as ISP. Costs are established at each site, there are no additional charges for the connection to the VPN.
ITA (proposed national system)	Not known at this time.
IRRIS	This would depend on the size of the deployment and which features the user would like installed. In essence, every hookup is a custom design. Fields from existing systems can be used to satisfy the needs of system users.
MobileShield™	There are only the infrastructure equipment costs.
ST-ISAC	For ST-ISAC this relates only to access to the secure website, which is not networked.
61. What is the cost to install the software per workstation?	
AIM	There is no cost per workstation. The system is paid for on a per user basis and requires only the usage of an internet browser.
DMIS	There is no cost to install the software at any workstation.
InfraGard	There is no cost to install InfraGard at any workstation.
ITA (currently developed prototype)	Same as 59.
ITA (proposed national system)	Not known at this time.
IRRIS	There are no separate workstations for IRRIS. Users only need access to the Internet and a Web browser.
MobileShield™	There are only the infrastructure equipment costs.
ST-ISAC	The cost at a member's installation is associated with the smart cards and the smart card readers. These are provided as part of the membership fee.
62. What is the annual cost of a maintenance agreement for the software with a two-hour response?	
AIM	The maintenance agreement is priced at 19.5% of the purchase cost. The response time ranges from 5 to 30 minutes and is available from 8:00 AM to 8:00 PM, Pacific Time.
DMIS	There is no maintenance agreement available.
InfraGard	InfraGard members are only required to sign the SAA, not a maintenance agreement. There are no maintenance costs passed on to users of InfraGard.
ITA (currently developed prototype)	No annual costs associated with the ITA prototype system.
ITA (proposed national system)	National ITA system not yet deployed and these requirements have not been established.

IRRIS	There is no standard pricing for IRRIS at this time, but the developer is willing to work with any interested agency.
MobileShield™	There is no set cost for a maintenance agreement at this time. The cost would be comparable to existing cellular network maintenance fees.
ST-ISAC	This is not applicable to ST-ISAC.
63. Does the maintenance agreement include 24/7 support from a telephone help desk?	
AIM	A 24/7-support service is available for 25% of the purchase price or at an hourly rate of $195 with a 2-hour minimum.
DMIS	There is no maintenance agreement available. However, there is a 24/7 help desk with a live person. For 14 hours per day, one may access the Help Desk personnel. For the remainder of the day, a network operator is available.
InfraGard	There is no maintenance agreement for InfraGard users; however, the Help Desk is available free of charge for 5 days a week, 12 hours a day. The hours have recently expanded to accommodate both East and West Coast users. Help Desk personnel are now available from 6:00 am to 11:00 pm, Central Time.
ITA (currently developed prototype)	The ITA prototype system has 24/7 technical support available through a help line.
ITA (proposed national system)	National ITA system not yet deployed and these requirements have not been established.
IRRIS	The signing of a maintenance agreement would be necessary for this option. There is no 24/7 help desk available now because the developer has not been approached on this topic yet. Currently, personnel are on-call to answer any important questions pertaining to IRRIS.
MobileShield™	Maintenance agreements have not yet been developed.
ST-ISAC	The cost of the membership includes 24/7 analytical and technical support.
64. If modifications are required to the software, at what hourly rate do you provide these services?	
AIM	Service is provided at a rate ranging from $160 to $195 per hour. Changes generally do not take too long. Small, medium and large modifications may cost close to $1,500, $5,000 and $15,000 respectively.
DMIS	The system has the current capability to make minor updates virtually automatically, although that is not yet current practice. It is expected that this feature may be activated soon.
InfraGard	This is not applicable to InfraGard.

ITA (currently developed prototype)	The ITA prototype system modifications are made free-of-charge.
ITA (proposed national system)	National ITA system not yet deployed and these requirements have not been established.
IRRIS	A cost schedule can be provided to anyone interested in IRRIS or an IRRIS-like system. Costs are based on the hourly rate (level) of the personnel involved. Standard rates are available.
MobileShield™	Costs are not yet determined to modify the equipment, if required. Costs would be negotiable.
ST-ISAC	This is not applicable to ST-ISAC.
65. Does the maintenance agreement provide for software upgrades without additional cost?	
AIM	Free upgrades are provided for in the agreement.
DMIS	There is no maintenance agreement but software upgrades are provided without charge.
InfraGard	There is no maintenance agreement for InfraGard and no additional cost to provide upgrades.
ITA (currently developed prototype)	The ITA prototype system upgrades are provided free-of-charge.
ITA (proposed national system)	National ITA system not yet deployed and these requirements have not been established.
IRRIS	It certainly can. The developer is upgrading IRRIS for MTMCTEA. There is no standard software agreement with the Military for IRRIS. The Military is usually willing to pay the upgrade costs. The developer provides the services and then calculates the cost for the Military. IRRIS is more of a customized project than a product.
MobileShield™	Costs are not yet determined if maintenance is required of the equipment. Costs would be negotiable.
ST-ISAC	This is not applicable to ST-ISAC. Any software upgrades would be to the secure website or associated systems and would not involve costs to the members above the annual fees.
66. What is the cost per user for on-site training on the use of the software system?	
AIM	Training fees are $150 per user with a minimum of 10 users.
DMIS	There is no charge for training, regardless of where delivered, but the budget to provide training is not unlimited. The system has embedded help as well as a paper operator's manual and user's guide. In general, most end-users are expected to train themselves using the *COG* [for Collaborative Operating Group, meaning organization] *Cookbook*, User's Guide, and embedded

	help functions. If there are unusual circumstances or needs, the developers will consider providing training assistance.
InfraGard	InfraGard does not offer on-site training. The Help Desk provides installation, setup, and training free of charge and on an as-needed basis.
ITA (currently developed prototype)	Users guide and training for the ITA Prototype System is provided at no cost.
ITA (proposed national system)	National ITA system not yet deployed and these requirements have not been established.
IRRIS	GeoDecisions standard hourly rates would also apply for on-site training regarding the use of IRRIS.
MobileShield™	Equipment-related training would be built into the price of the product.
ST-ISAC	Training costs, if any, are presumed to be quite small.
67. To attain full functional use of the software, does one have to purchase additional licenses for software systems?	
AIM	No additional licenses need to be purchased for full functionality.
DMIS	No additional licenses need to be purchased for full functionality.
InfraGard	No additional licenses need to be purchased for full functionality.
ITA (currently developed prototype)	Not for the ITA prototype system.
ITA (proposed national system)	National ITA system not yet deployed and these requirements have not been established, but would expect that all software and such will be provided as needed.
IRRIS	To attain full functional use of the system, one has to purchase additional licenses for the software systems, but the developer would provide a one-stop shop and provide the user with a total cost for everything.
MobileShield™	To attain full functional use of the system, one has to purchase additional licenses for software systems.
ST-ISAC	The extensive use of secure email by ST-ISAC makes a small investment (approximately $50.00) in a secure email service desirable, though not, strictly speaking, necessary.
68. Can system access be differentiated by user profile?	
AIM	The system can be differentiated by user profile.
DMIS	The system access can be differentiated by user profile.
InfraGard	Yes. Access to the InfraGard system is differentiated by a user profile that is determined after the user has successfully completed the security background checks conducted by the FBI.
ITA (currently developed	In the ITA prototype system access management through user password and physical access to the system.

prototype)	
ITA (proposed national system)	National ITA system not yet deployed and these requirements have not been established.
IRRIS	Yes. Access to IRRIS is differentiated by a user profile. Individual users have different levels of access to various subsets of data within IRRIS.
MobileShield™	System access can be differentiated by user profile. Access priorities can be defined.
ST-ISAC	Classes of users do exist. Given the different modal profiles, not all users have access to the same information. The capability exists to establish an infinite number of member access classes.
69. Does the system track and log the origin (person and agency) of the data?	
AIM	Every single creation or modification is stored.
DMIS	Yes, the system tracks and logs the origin of the data.
InfraGard	The system can track the user ID. From the user ID, one would require access to the user database to determine the identity of the user. Also, every computer has a unique address to access the Web called an Internet Protocol (IP). This requires positive identification of the user. Therefore, when a user is logged on to the Internet (using any application, including InfraGard), the user can be tracked. The InfraGard system does not currently log the time of use by a specific user.
ITA (currently developed prototype)	Yes, under the ITA Prototype System.
ITA (proposed national system)	National ITA system not yet deployed and these requirements have not been established.
IRRIS	Yes. The origin of the data and users are both logged. Furthermore, the same user cannot be logged into the site from two different places. IRRIS records and logs all activities of every user on the site, but the developer chooses not to monitor these activities unless system records need to be tracked for a specific reason.
MobileShield™	The system tracks and logs the origin (person and agency) of the data.
ST-ISAC	This would only apply to discussion forums and postings, since otherwise, members would have little capability to post information, except by phone or secure email in which they, presumably, would not be anonymous, at least not to EWA, the day-to-day operator of the system.. The authentication system tracks access and specific utilization.
70. Are users timed out for inactivity?	
AIM	Users are timed out for inactivity and the customer can set that

	time limit.
DMIS	Yes, various timeouts exist for different things.
InfraGard	No, but the capability exists and can be installed that way.
ITA (currently developed prototype)	Yes, the ITA prototype system uses time activated Screen saver functions that are password access controlled.
ITA (proposed national system)	National ITA system not yet deployed and these requirements have not been established.
IRRIS	Yes. IRRIS logs out users after 10 minutes of inactivity.
MobileShield™	Users can be timed out for inactivity.
ST-ISAC	Yes, the timeout is adjustable. Users are removed from the service when the Smart Card is removed from the reader.
71. Are there other safeguards invoked by the software to protect the security of the information displayed if the operator leaves their workstation?	
AIM	There are no other safeguards invoked by the software to protect the security of the information displayed if the operator leaves their workstation.
DMIS	No, there is no provision for anything like this.
InfraGard	No, not at this time. However, the VPN of the system is certified and accredited by the FBI.
ITA (currently developed prototype)	Same as 70.
ITA (proposed national system)	National ITA system not yet deployed and these requirements have not been established.
IRRIS	Processes monitor the log files created to detect any intrusion or unauthorized access. Everything is recorded for security purposes. Firewalls are a major part of the system.
MobileShield™	There are no other safeguards invoked by the system to protect the security of the information displayed if the operator leaves their workstation.
ST-ISAC	The website is inaccessible when the Smart Card is removed from the reader.
72. Does the system use lengthy alphanumeric passwords?	
AIM	The system can be set to use whatever requirements are desired.
DMIS	Yes, with the latest update, nine character passwords are mandatory.
InfraGard	Yes, each password is eight characters.
ITA (currently developed prototype)	Yes, the ITA Prototype System uses alphanumeric passwords.
ITA (proposed national system)	National ITA system not yet deployed and these requirements have not been established.

IRRIS	Yes, the password must be at least eight characters and must use at least one letter, one digit, and one special character.
MobileShield™	The system uses lengthy alphanumeric passwords.
ST-ISAC	Yes, the system uses lengthy alphanumeric passwords.
73. Are there limitations on the period of time during which a password may be validly used before it must be changed?	
AIM	There are limitations and the customer can set the limits.
DMIS	This is a decision for each system administrator.
InfraGard	Starting September 1, 2003, when the SSL system is deleted, users will be required to change their passwords every 90 days. They will be required to verify their names, addresses, and that they are still working for the same company.
ITA (currently developed prototype)	Each ITA Prototype System site administrator determines the amount of time for passwords to be changed.
ITA (proposed national system)	National ITA system not yet deployed and these requirements have not been established.
IRRIS	Yes, system passwords must be changed every 90 days.
MobileShield™	There are limitations on the period of time during which a password may be validly used before it must be changed.
ST-ISAC	Yes, there are limitations on the period of time during which a password may be validly used before it must be changed.
74. Are there limitations on the number of times a password can be used before it becomes invalid?	
AIM	There are no limitations on the number of times a correct password can be used.
DMIS	Currently, password changes are not forced on end-users. However, with the shift to more robust passwords, that is expected to be invoked shortly.
InfraGard	There are currently no limitations on the number of times a password can be used, however, InfraGard will only allow a single user to be on one module at a time. The system will allow the user access to the new module, but will automatically time out the user's access on the old computer as soon as he or she is logged onto the new module.
ITA (currently developed prototype)	In the ITA Prototype System, limitations can be set by the site administrator.
ITA (proposed national system)	National ITA system not yet deployed and these requirements have not been established.
IRRIS	The same password may not be used twice in a row.
MobileShield™	There are limitations on the number of times a password can be used before it becomes invalid.

ST-ISAC	There are no limitations on the number of times a correct password can be used.
75. Are there limitations on the number of times the use of an incorrect password may be attempted?	
AIM	This limitation can be implemented with the system.
DMIS	No, there are currently no limitations on how many times an incorrect password may be attempted.
InfraGard	Yes, three attempts and then the user will become locked out of the system. Then, the user must physically contact the Help Desk to regain access. A security check will be conducted again before the Help Desk can provide the user with his or her correct password.
ITA (currently developed prototype)	The ITA Prototype System does have this capability and is enabled. Number of actual tries is a matter of security that cannot be released.
ITA (proposed national system)	National ITA system not yet deployed and these requirements have not been established.
IRRIS	Yes, three times.
MobileShield™	There are limitations on the number of times the use of an incorrect password may be attempted
ST-ISAC	There are limitations on the number of times the use of an incorrect password may be attempted.
76. Are there internal system alerts for suspicious system, network, or database activity?	
AIM	AIM does contain internal system alerts for suspicious system activity.
DMIS	Yes, there is a variety of intrusion detection, intrusion denial and monitoring provisions. FEMA has tested the security of the system and found it to be acceptable.
InfraGard	Security is monitored by a private contractor that maintains the secure socket layers, firewalls, and passwords. They also scan for viruses and worms on a routine basis.
ITA (currently developed prototype)	Yes, for the ITA Prototype System.
ITA (proposed national system)	National ITA system not yet deployed and these requirements have not been established.
IRRIS	Yes. Many processes monitor the log files to detect any unauthorized access.
MobileShield™	There are internal system alerts for suspicious system, network or database activity. The system has *denial of service* capability. It can see a hack occurring and not only prevent it, but trace where it is coming from.
ST-ISAC	Yes, there are extensive monitoring tools in place.

END-USER FEATURES MATRIX

Table 4 is the End-User Features Matrix. It includes each of the questions asked along with the respective responses provided by the interviewee end-user of the software system. The presentation approach allows the reader to compare the response provided by each system end-user. This should assist in the determination of which software system satisfies the greatest number of requirements established by the potential user.

Note that the responses provided were those obtained during the interviews. Verification of the information received and testing of the capabilities documented were beyond the statement of work associated with this Task Order.

In the case of the ITA software system, an end-user was asked to fill out the respective questionnaire matrixes directly without the use of an interviewer. The posted ITA responses are as received except when necessary to correct spelling or grammatical errors and to provide for a consistent presentation of the materials across all software systems. This approach was used for a number of reasons including: in a previous activity within the Task Order the Team had evaluated several competency areas associated with the ITA system and were therefore somewhat familiar with that earlier version as opposed to the current version; and the Team did not want their previous experience with the software system to influence in any way the words that were recorded during the interview and eventually posted in the Features Matrixes.

It is strongly urged that before any of these systems are acquired or purchased that they should be thoroughly tested by the potential user in their then current environment or a similar environment and that functional specifications regarding the actual capabilities of the desired software system be comprehensively developed and included in the procurement bid package used by the procuring agency. The information presented here is simply a snapshot of the selected systems at the point in time of the data collection process and that no verification of the acquired information or testing of the systems was accomplished as part of the requirements of the statement of work associated with this Task Order.

THREE ADDITIONAL SYSTEMS CONSIDERED

The Senior Program Officer (SPO) for the NCHRP Secure Communication Infrastructure Task Order participated in the *Summit on Interoperable Communications for Public Safety* in Gaithersburg, MD during June 26-27, 2003. At this summit, sponsored by the National Institute of Standards and Technology (NIST), approximately 60 existing communication systems were considered. Perusal of the available information on the systems revealed three that may have merit with respect to the exchange of security-related information within the transportation industry. These systems are:

- ❒ Global Justice Information Sharing Initiative (Global);
- ❒ Organization for the Advancement of Structured Information Services (OASIS); and
- ❒ Regional Information Sharing Systems (RISS).

TABLE 4: END-USER FEATURES MATRIX

1. What is the overall business function of the division within the organization in which this software operates?	
AIM	The function of the USDOT Crisis Management Center (CMC)[27] is to undertake crisis management activities such as transportation alerts and early warnings.
DMIS	The interviewed organization is assigned to the Department of

[27] The CMC was previously known as the Transportation Information Operations Center (TIOC).

	Homeland Security, a branch of the pre-positioning systems command for a military branch.
InfraGard	This division of law enforcement serves as an outreach function of the cyber crime squad. At one point, the focus of the division regarded physical terrorism, but now the focus is on detecting cyber crime.
ITA (currently deployed prototype)	This section is responsible for emergency operations. A second unit is expected to be established in a part of the organization that is manned on a 24-hour basis, 7 days per week.
IRRIS	There are three programs of national defense: highways, railroads, and ports. The business function of the Military Traffic Management Command Transportation Engineering Agency (MTMCTEA) is to ensure that these programs have adequate design and capability to support national defense and other military-related issues. The business function of the Military Traffic Management Command Operations (MTMC Ops) center is to support the real-time surface transportation of the military community. This entails all aspects of freight management, including booking and monitoring shipments. The MTMC Ops center is currently using IRRIS as a freight management tool, whereas MTMCTEA is using it as an infrastructure tool.
MobileShield™	The focus of the division is in the areas of Homeland Security, law enforcement and first responders.
ST-ISAC	Division is responsible for information management, information assurance, disaster recovery, quality programs, and change management.
2. How long has your organization been using the (software) system?	
AIM	AIM has been used for one year.
DMIS	The organization has been using all versions of the system since its conceptual inception.
InfraGard	The Philadelphia InfraGard Chapter of the FBI has been using the system since it was piloted in 1998. Its inception became official in 1999.
ITA (currently deployed prototype)	The interviewed organization was one of the first users and participated in the first demonstrations in July 2002.
IRRIS	MTMCTEA has been using IRRIS since March 1999. MTMC Ops has been using it since December 2001.
MobileShield™	The organization has been using the software for 18 months in a demonstration capacity.
ST-ISAC	Organization has been using ST-ISAC since its inception, about two years ago.
3. For what length of time has the end-user interviewed had personal	

experience in using the software?	
AIM	The interviewed end-user has used AIM for 10 months.
DMIS	The end-user interviewed is not currently personally using the system but has had involvement with the system since its conceptual inception.
InfraGard	The two interviewed end-users of InfraGard have been using the system since November 2000 and since its research phase in 1998.
ITA (currently deployed prototype)	The interviewed end-user was one of the first users and participated in the first demonstration in July 2002.
IRRIS	The interviewed end-user has been using IRRIS since March 1999.
MobileShield™	The interviewed end-user has used MobileShield™ for one month.
ST-ISAC	The interviewed end-user has been using ST-ISAC since its inception, about two years ago.
4. On how many workstations is your organization currently running the software?	
AIM	Twenty-five workstations in the CMC use the AIM system.
DMIS	The interviewed organization currently runs DMIS on two workstations but is in the process of expanding it to six workstations.
InfraGard	InfraGard does not require separate workstations, as it is attached to the network. Two laptops within the Philadelphia chapter have separate dial-up connection capabilities for users to log-on to the InfraGard website and their email accounts.
ITA (currently deployed prototype)	Only one unit is being used at this time. Two units are located at the same location, one is the primary and the other the back up.
IRRIS	IRRIS is available on every workstation, as it is Internet-based. All that is needed for IRRIS to run is an Internet connection and a Web browser.
MobileShield™	The system is being used in a demonstration capacity, currently on two mobile workstations.
ST-ISAC	Access to the secure website is provided through five workstations. Unless the member wishes to pay more, five card-reading workstations is the standard configuration.
5. Describe the functions the (software) system performs for your organization.	
AIM	The system enables the Center to establish daily duty logs recording all activity, produce Incident and Situation Reports, produce Alert Bulletins, and distribute information to pertinent individuals.

DMIS	The program produces great visual images, particularly using geospatial images with overlays in maps. It can also be interactive, with many things moving on it. For the TOPOFF2 exercise, in which the interviewed organization participated, use was made of the ability to monitor live video feed.
InfraGard	InfraGard serves as a liaison and outreach to private industry. The Philadelphia chapter has an independent web page in which it can post information. The FBI coordinators the Philadelphia chapter and conducts membership processing. These coordinators also provide: ❒ member statistics; ❒ marketing web pages; ❒ guidelines for press releases; ❒ application information; and ❒ letter writing techniques.
ITA (currently deployed prototype)	The interviewed organization feels that they have not used it as effectively and efficiently as they would have liked. They use it for secure communications and sharing of disaster information as needed.
IRRIS	For MTMCTEA, IRRIS provides infrastructure data and real-time information regarding events across the United States, including weather, traffic, construction, special events (e.g., Olympic Games, concerts, football games, as well as emergency-related incidents), congestion tracking information, and more. For MTMC Ops, IRRIS has replaced numerous phone calls and faxes by providing a user-friendly tracking system to monitor manual freight shipments. An economic evaluation was conducted, and the results revealed that MTMC Ops saved over $10 million last year in operations costs by using IRRIS.
MobileShield™	Interoperability is the single most critical function that the system affords. Voice data and video interaction is possible with anything that can have an IP address, such as a PDA, a cell phone, a video camera, or a LMR.
ST-ISAC	ST-ISAC performs standard alert monitoring, classification, evaluation and distribution of alerts. The railroad now routinely turns over items to ST-ISAC on the basis of anomalous appearance, asking the analytical staff at ST-ISAC to evaluate it and compare with anything they recognize going on in the industry. They also use ST-ISAC as a conduit to the Joint Terrorism Task Force (JTTF) and the Department of Homeland Security (DHS).
6. What version of the software is your organization currently running?	
AIM	This was not known by the interviewed end-user.
DMIS	The interviewed organization is using the latest version of the

	software, issued in June 2003.
InfraGard	The latest VPN used by InfraGard is called SmartPass. The interviewed users were unaware of the specific version of the software currently being used by their chapter.
ITA (currently deployed prototype)	The interviewed organization is using version 2.3a.
IRRIS	Version 4.3.5. MTMC encourages the developers to make changes almost weekly. MTMC is a rapid response organization. Initially, new major versions of IRRIS were planned to come out every six months, but now they are done almost every three months. Minor upgrades are conducted almost weekly. Additionally, when more users sign onto IRRIS, more customized changes are required.
MobileShield™	The software system is in demonstration capacity. The version is unknown.
ST-ISAC	This is not applicable to ST-ISAC.
7. Are there any additional modules beyond the core version of the software that your organization has chosen to acquire?	
AIM	There are no additional modules beyond the core version of the software that the CMC has chosen to acquire.
DMIS	This question is not applicable to DMIS as the identical, complete package is delivered to all end-users. Nonetheless, the interviewed organization has made most use of the instant messenger and journal entry functions of the software.
InfraGard	The interviewed end-users are unaware of any additional modules that exist beyond the core version of the InfraGard system. However, the InfraGard developers and managers have made mention of future options, such as: sharing files; instant messaging; and other additional capabilities.
ITA (currently deployed prototype)	This is not applicable to ITA.
IRRIS	IRRIS has four to five years worth of improvements coming. IRRIS Light serves as a tool for navigation and other crucial functions in an austere environment. IRRIS To Go is a broad bandwidth PDA-type device that allows the user to download maps and queries in real-time. Robust routing will be available in the middle of July (2003) and a more robust alerting system will also be provided online in the near future. Plans to install the classified version of IRRIS, similar to the military's Secret Internet Protocol Router Network (SIPRNET), are in the works. MTMC is also looking into tracking tactical areas, not just forts and ports.
MobileShield™	There are no additional modules beyond the core version of the software that the organization has chosen to acquire.

ST-ISAC	This is not applicable to ST-ISAC.
8. When were the additional modules purchased? At the same time as the core version of the software or at a later date?	
AIM	This is not applicable to AIM.
DMIS	This is not applicable to DMIS.
InfraGard	This is not applicable to InfraGard.
ITA (currently deployed prototype)	This is not applicable to ITA.
IRRIS	Additional modules do not need to be purchased. IRRIS is completely Internet-based. Once a user is connected to the system, all of the services are free. IRRIS compartmentalizes who has access to the system. The security group at MTMC issues all user identifications and passwords. The philosophy of IRRIS is that everyone should try to gain advantage by leveraging off of other people's work. By partnering with the Coast Guard, MTMC is paid to add the information that the Coast Guard would like to see about water layers. Then, everyone is able to benefit from the available data. However, tracking information is very limited. Users must be on a *need-to-know* basis and have a security clearance to gain access to tracking information. MTMC has offered some individuals a 60-day account, but MTMC security group prefers to limit the use of IRRIS as much as possible.
MobileShield™	This is not applicable to MobileShield™.
ST-ISAC	This is not applicable to ST-ISAC.
9. What value has been found from the additional modules?	
AIM	This is not applicable to AIM.
DMIS	This is not applicable to DMIS.
InfraGard	This is not applicable to InfraGard.
ITA (currently deployed prototype)	This is not applicable to ITA.
IRRIS	Each previously mentioned IRRIS module is available in some form at this current time. For instance, the email alert system can send emails, if a user chooses to set up the account that way, without him/her ever having to log onto IRRIS. Specific, customized reports could be generated for this purpose and emailed directly to the user. IRRIS is also able to monitor crucial data, if one chooses to have the system do so. IRRIS should be used to monitor and analyze everything because the system does not become bored. There is no need to even check the website, unless an alert provides a direct link to the user for the IRRIS site.

MobileShield™	This is not applicable to MobileShield™.
ST-ISAC	This is not applicable to ST-ISAC.
10. What has been the experience with the software's stability and reliability?	
AIM	The system is reliable. The one issue that the interviewed end-user noted was occasional login difficulties.
DMIS	It has been good, not great, at least historically. Early versions of the software were an attempt to disseminate something quickly, without necessarily having a perfect product. It is probable that the most recent version is more reliable.
InfraGard	Specific members of the InfraGard managing staff are very efficient. Also, the Help Desk, staffed by students attending LSU, is available as a helpful resource. The interviewed users have expressed some issues with the entry-level experience of the Help Desk personnel, but they agree that all problems seem to be resolved instantly. Although the initial setup took about a week, once the system was up and running, there have been very few problems, according to the interviewed end-users.
ITA (currently deployed prototype)	The interviewed organization has had some problems with the *send message* function and with it locking up while redrawing the time line cone. These and some other minor bugs have been addressed and solved or a work-around procedure has been used.
IRRIS	It is extremely reliable. In three years, the system has only been down a couple of times. Maintenance is performed on a monthly basis, and the system is unavailable for about an hour during each session. Maintenance is usually conducted on the weekend and advanced notice is sent to all users. Due to the recent war in Iraq, IRRIS was used all over the world, including at the Pentagon Operations Center.
MobileShield™	The product is extremely reliable, and no "breakage in signal" has been observed.
ST-ISAC	There has been no failures to-date, so there has been 100 percent availability of the system.
11. What opinions predominate with regard to the (software) system's general user-friendliness?	
AIM	The interviewed end-user gave AIM a grade of B+ for its user-friendliness. AIM was said to be fairly forgiving with user mistakes. One example of difficulty is the occasional problems that arise when a user attempts to delete a document that he or she incorrectly created.
DMIS	User friendliness is thought to be very high. In the assessment of the interviewed end-user, the system is virtually intuitive. The developers call this "big buttons."

InfraGard	The interviewed end-users expressed that the system is very user-friendly. Once granted access to the site, navigation is simple. The support functions are not as smooth as they could be, but new membership processing, from a coordinator's standpoint, has improved greatly. It is also easy to acquire member statistics. A majority of InfraGard's members simply attend chapter meetings and are not users of the secure Internet system. Some chapters really support their coordinators and that certainly contributes to the system's overall success. The membership is representative of a broad range of private industries, which includes everything from global companies to mom-and-pop proprietorships. The interviewed end-users perform much of the administrative work associated with membership processing.
ITA (currently deployed prototype)	Some new features and fixes have made it better, but like any software, it is changing and getting better with age.
IRRIS	The interviewed end-user described IRRIS as a great system. Perhaps it is more difficult than the average website, but it requires little or no training. The zoom feature is slightly complicated. The interviewed end-user said that he does not think there is a way to make the system any easier to comprehend.
MobileShield™	The system is very user-friendly because the infrastructure provided by the MobileShield™ system allows people to use the equipment that they are already familiar with. User-friendliness shortcomings are dependent on the natural user-unfriendliness of a user's device of choice.
ST-ISAC	It is fine. The secure website is not used as much as other features of ST-ISAC, just used for posting information, so the system's user-friendliness may not be much of an issue.
12. Describe the usefulness of developer-provided documentation.	
AIM	AIM's manual is saved on the desktop of every workstation in the CMC. The document is detailed and comprehensive.
DMIS	The interviewed end-user has seen a version of the documentation, but not recently.
InfraGard	A user manual was not provided to the interviewed end-users. When the software was received, a listing of steps on how to set up InfraGard and contact the Help Desk was provided. This was helpful. The FBI developers used to send out a CD-ROM for the VPN software. It was just like loading any software package. Documentation was provided that listed a few steps for installation, which was much like loading new camera software. A welcome letter from the program manager accompanied this CD-ROM. The interviewed end-users concluded that this

	documentation must have been sent only during the test phase. Documentation on the website is very straightforward. The tabs, located on the side of each page, help the user negotiate the information he or she would prefer to view.
ITA (currently deployed prototype)	The interviewed organization has not used it much, but they think that the documentation seems to be well written.
IRRIS	The interviewed end-user believes that, in general, documentation is a waste of time and money. MTMC provides minimum documentation. The company's focus is on results. Instruction manuals and other system documents are outdated almost as soon as they are printed. There is a short video (about 12 minutes) that provides an overview of IRRIS's capabilities. The system also offers a very helpful *how-to* function that is similar to the Microsoft help function (paperclip).
MobileShield™	The end-user interviewed was not aware of any developer-provided documentation.
ST-ISAC	The documentation has primarily been oriented toward how to install the smart card rather than how to use the website, which may be appropriate, given the system's simplicity.
13. Describe the value of the software system's help functions.	
AIM	The software does contain help functions. The value of these functions, however, is impossible to determine due to the fact that none of the CMC staff uses them.
DMIS	The interviewed end-user has had no recent personal experience with the help function.
InfraGard	Specific members of the InfraGard managing staff perform the help function most efficiently. The Help Desk is a great compromise, as it provides free support while training LSU students. The students are very professional, but can consume time during the learning curve. Many times, they require assistance form their managers to successfully solve an issue.
ITA (currently deployed prototype)	The interviewed organization has not used the help function.
IRRIS	The interviewed IRRIS end-user feels that the help function of the system is very user-friendly. It offers the same topics as any standard software set and more. Users can type in key words and locate information about particular help topics. There is a troubleshooting option and a complete tutorial.
MobileShield™	The system has no help functions.
ST-ISAC	In general, there are few help functions. It might be helpful to understand better the distinction between anonymous and attributable reports.

14. Did your organization engage in formal training for personnel using the software system?	
AIM	No formal training was given; however, informal training such as learning from a coworker was how the staff at CMC gained their AIM knowledge.
DMIS	The interviewed organization used informal, not formal training.
InfraGard	No formal training is provided for InfraGard's members. It is not really necessary, as many of the members are familiar with basic Internet functions. The coordinators of the system, however, are required to train for a week regarding the capabilities of InfraGard and their responsibilities.
ITA (currently deployed prototype)	The interviewed organization did engage in formal training for personnel using the system.
IRRIS	No, it was not necessary. MTMC recommends that all users see the 12-minute overview video. It is available on the Web and on CD-ROM.
MobileShield™	The organization did not engage in formal training for personnel using the system.
ST-ISAC	No, there was no formal training conducted.
15. How much formal training was provided for personnel using the software system?	
AIM	This is not applicable to AIM.
DMIS	This is not applicable to DMIS.
InfraGard	As previously stated, there is no formal training available for end-users. Instructions are sent to the users via a welcoming email, provided by a key member of InfraGard's management staff, once the user has been approved to access the system.
ITA (currently deployed prototype)	One day of training was needed for personnel using the software.
IRRIS	This is not applicable to IRRIS.
MobileShield™	This is not applicable to MobileShield™.
ST-ISAC	This is not applicable to ST-ISAC.
16. Did the formal training received prepare users for utilizing the (software) system?	
AIM	This is not applicable to AIM.
DMIS	This is not applicable to DMIS.
InfraGard	This is not applicable to InfraGard.
ITA (currently deployed prototype)	The feeling of the interviewed organization was that users who had received the formal training were mostly prepared.

IRRIS	This is not applicable to IRRIS.
MobileShield™	This is not applicable to MobileShield™.
ST-ISAC	This is not applicable to ST-ISAC.
17. How long was it before individuals were able to competently use the software system?	
AIM	Users feel confident after two days of system usage.
DMIS	The interviewed end-user was unsure.
InfraGard	Almost immediately.
ITA (currently deployed prototype)	The system has not been fully implemented, so the question cannot be answered at this time. The interviewed organization feels that it must move this application to a permanent 24/7 office and then reevaluate.
IRRIS	MTMC would say 12 minutes, but it probably takes about an hour of working with IRRIS's functions to really learn the system. Within a day, users can practically do anything. Users must be able to use the Internet. If a user does not understand the Internet, IRRIS can be very complicated. IRRIS developers assume that the users of the system have some basic understanding of the Internet.
MobileShield™	New users are immediately able to competently use the system. Users can use communication devices that they are accustomed to using.
ST-ISAC	New users were able to competently use the system immediately.
18. Has any developer-provided customer support been used?	
AIM	No developer-provided customer support has been used.
DMIS	The interviewed organization uses customer support every day.
InfraGard	The interviewed end-users expressed that they contact InfraGard's management staff several times a week to coordinate membership processing. A general user does not usually need to contact the management staff or Help Desk on a regular basis.
ITA (currently deployed prototype)	Yes, customer support has been used.
IRRIS	Yes. There is an in-house expert available at MTMC to help with IRRIS concerns. The product is always changing. Some software systems have development curves, but IRRIS has not been sustained for any length of time. If customers call and say they need a, b, and c, IRRIS developers are willing to modify the system usually within a couple of weeks. As long as funding is available, IRRIS will continue to improve and expand its functionality on a frequent basis. There is a major push right now for arms and ammunition. MTMC keeps the developer in constant contact with its major customers. Direct contact, with no

	government liaison, has resulted in strong relationships among customers who simultaneously support IRRIS.
MobileShield™	The interviewee has not used any developer-provided customer support.
ST-ISAC	Yes, customer support has been used periodically.
19. Was using developer-provided customer support effective in resolving problems?	
AIM	This was not applicable to AIM.
DMIS	The interviewed end-user indicated that it was effective in resolving *his* problems.
InfraGard	Yes, the staff is very effective in resolving problems and satisfying requests.
ITA (currently deployed prototype)	Yes, the customer service provided was effective in resolving problems.
IRRIS	Yes, customer service of IRRIS has been very effective.
MobileShield™	This was not applicable to the MobileShield™.
ST-ISAC	Yes, the customer service provided was excellent.
20. Has the software fulfilled *its originally promised purpose*?	
AIM	It has fulfilled its originally promised purpose. The software has provided CMC with the ability to create logs of incidents, create incident reports and distribute them, as hoped.
DMIS	This has been constrained, somewhat, by available funding. The interviewed end-user feels that the current version is about 75 percent of what was originally desired.
InfraGard	The interviewed end-users feel that InfraGard has fallen short of what it originally promised, but it has grown beyond the initial anticipated member status (8,000 secure members).
ITA (currently deployed prototype)	Yes, the software has fulfilled its originally promised purpose.
IRRIS	It has exceeded in every aspect. A contractor was hired to develop IRRIS. The contractor has always finished ahead of schedule, under budget, and has always exceeded what MTMC expects. This is why MTMC allows the developer to work directly with IRRIS customers.
MobileShield™	The software has fulfilled its originally promised purpose.
ST-ISAC	Yes, ST-ISAC has done a wonderful job. It has been one single place to get information. There have been some problems with persuading railroad members to give information, but this has nothing to do with the structure of the system.

21. In what ways has the software not fulfilled its originally promised purpose?	
AIM	This question is not applicable to AIM.
DMIS	This question is not applicable to DMIS.
InfraGard	InfraGard's original goal was to provide an avenue for two-way communication to occur between the private sector and the FBI. It has not achieved this goal because the FBI is disseminating most of the information, while many private industry users are not relaying their critical information to the FBI. InfraGard has not been able to streamline the influx of communication from the private sector. InfraGard was built on establishing trust within the private industry. The system has improved relationships and encouraged the exchange of information, but it has not fully bridged the gap between private industry and the FBI. InfraGard is a valuable asset, as it exists now. Its focus, however, is different than was originally planned. Alerting private industry of security threats has been successful and communications with private industry have tremendously improved. The original goal of InfraGard assumed that private industry would respond by providing critical information. There is evidence that relationships are being fostered and trust is being built. It is a "trickle," according to the interviewed end-users, but it seems that open communication will slowly, but eventually, become a reality among private industry members.
ITA (currently deployed prototype)	This question is not applicable to ITA.
IRRIS	This question is not applicable to IRRIS.
MobileShield™	This question is not applicable to MobileShield™.
ST-ISAC	This question is not applicable to ST-ISAC.
22. What was the original purpose for which the (software) system was acquired?	
AIM	This question is not applicable to AIM.
DMIS	This question is not applicable to DMIS.
InfraGard	The original purpose of InfraGard was to provide an avenue in which two-way communication could occur between private industry and the FBI.
ITA (currently deployed prototype)	This question is not applicable to ITA.
IRRIS	This question is not applicable to IRRIS.
MobileShield™	This question is not applicable to MobileShield™.
ST-ISAC	This question is not applicable to ST-ISAC.
23. Has the business function of the division using the (software) system	

changed since it was acquired?	
AIM	This question is not applicable to AIM.
DMIS	This question is not applicable to DMIS.
ITA (currently deployed prototype)	This question is not applicable to ITA.
InfraGard	Yes.
IRRIS	This question is not applicable to IRRIS.
MobileShield™	This question is not applicable to MobileShield™.
ST-ISAC	This question is not applicable to ST-ISAC.
24. In what ways has the division's function changed?	
AIM	This question is not applicable to AIM.
DMIS	This question is not applicable to DMIS.
InfraGard	The focus changed from counterterrorism to cyber crime.
ITA (currently deployed prototype)	This question is not applicable to ITA.
IRRIS	This question is not applicable to IRRIS.
MobileShield™	This question is not applicable to MobileShield™.
ST-ISAC	This question is not applicable to ST-ISAC.
25. Has the software performed as originally *expected*? (To Developer)	
AIM	This question is not applicable to AIM.
DMIS	This question is not applicable to DMIS.
InfraGard	No.
ITA (currently deployed prototype)	This question is not applicable to ITA.
IRRIS	This question is not applicable to IRRIS.
MobileShield™	This question is not applicable to MobileShield™.
ST-ISAC	This question is not applicable to ST-ISAC.
26. In what ways has the software not performed as originally *expected*? (To Developer)	
AIM	This question is not applicable to AIM.
DMIS	This question is not applicable to DMIS.
InfraGard	It has not fulfilled its originally promised purpose.
ITA (currently deployed prototype)	This question is not applicable to ITA.
IRRIS	This question is not applicable to IRRIS.
MobileShield™	This question is not applicable to MobileShield™.
ST-ISAC	This question is not applicable to ST-ISAC.
27. Has the software performed as originally *expected*? (To User)	

AIM	The software has not disappointed the users at CMC.
DMIS	Yes, the software has performed as envisioned.
InfraGard	This question is not applicable to InfraGard.
ITA (currently deployed prototype)	Yes, the system has performed as expected.
IRRIS	Yes, the system has performed as expected.
MobileShield™	Yes, the system has performed as expected.
ST-ISAC	Yes, the system has performed as expected.
28. In what ways has the software not performed as originally *expected*? (To user)	
AIM	This question is not applicable to AIM.
DMIS	This question is not applicable to DMIS.
InfraGard	This question is not applicable to InfraGard.
ITA (currently deployed prototype)	This question is not applicable to ITA.
IRRIS	This question is not applicable to IRRIS.
MobileShield™	This question is not applicable to MobileShield™.
ST-ISAC	This question is not applicable to ST-ISAC.
29. Describe how the software system was originally expected to perform.	
AIM	This question is not applicable to AIM.
DMIS	This question is not applicable to DMIS.
InfraGard	This question is not applicable to InfraGard.
ITA (currently deployed prototype)	This question is not applicable to ITA.
IRRIS	This question is not applicable to IRRIS.
MobileShield™	This question is not applicable to MobileShield™.
ST-ISAC	This question is not applicable to ST-ISAC.
30. Has the business function of the division using the (software) system changed since it was acquired?	
AIM	This question is not applicable to AIM.
DMIS	This question is not applicable to DMIS.
InfraGard	This question is not applicable to InfraGard.
ITA (currently deployed prototype)	This question is not applicable to ITA.
IRRIS	This question is not applicable to IRRIS.
MobileShield™	This question is not applicable to MobileShield™.
ST-ISAC	This question is not applicable to ST-ISAC.
31. In what ways has the division's function changed?	

AIM	This question is not applicable to AIM.
DMIS	This question is not applicable to DMIS.
InfraGard	This question is not applicable to InfraGard.
ITA (currently deployed prototype)	This question is not applicable to ITA.
IRRIS	This question is not applicable to IRRIS.
MobileShield™	This question is not applicable to MobileShield™.
ST-ISAC	This question is not applicable to ST-ISAC.
32. Describe your experience with the software when connecting with all other users of the system both internal and external.	
AIM	The software has not been a problem. However, issues have arisen due to *user errors*. For example, some users have opened a new duty log for every incident. During a crisis, one does not have time to check for user errors. Users that understand the procedure would not create this issue.
DMIS	The interviewed end-user was unsure about the direct experiences, connecting with other users.
InfraGard	Many of the Philadelphia chapter members are not secure users. InfraGard is designed to disseminate information via email to the membership in “one foul swoop,” according to the interviewed end-users. If it is determined that the information is of a nature that both groups (secure and non-secure) need to know, coordinators will send the information to all members. The connection to non-secure users can be made possible through an everyday email account.
ITA (currently deployed prototype)	The only problem encountered by the interviewed organization was with the delivery of messages. They would always include themselves on messages sent. Sometimes these messages did not return to them.
IRRIS	It is completely Internet based. All users are offered the same information at the same time. If users are using various databases, they may sometimes receive different or conflicting information. This is because they are not using a central master database. Local databases can become out-of-date. IRRIS can provide Excel spreadsheets of information. Having a central master database makes the data very reliable and everyone has the same information. It is also easier to maintain. MTMC consistently updates its road network every time Navtec sends out an upgrade.
MobileShield™	During the demonstration process, at most five users have been connected. Connectivity was not an issue.
ST-ISAC	Primarily, connection to other users has not taken place through ST-ISAC but rather by teleconference or in face-to-face meetings

	as part of the working group.
33. Describe the timeliness with which the system has delivered information.	
AIM	The system delivers the information in seconds. The system is as fast as a user on the system.
DMIS	There was some problem, during TOPOFF2, with transmitting near-real time video. The bandwidth was a constraint.
InfraGard	According to the interviewed end-users, when the information concerned threats such as viruses and worms, private industry would routinely say, "By the time we get the info, it is not valid anymore." This is a product of how the information is communicated and collected. When humans are involved, it slows the process down. Immediately following the events of 9/11, communication became very timely. Since then, the rush of information has tapered.
ITA (currently deployed prototype)	The system appeared to get messages through quite quickly once the address book was cleaned up.
IRRIS	Most IRRIS queries are answered within a few minutes, maybe even a few seconds. However, there are times when some queries [e.g., Meals Ready to Eat (MRE) inquiries] can take 20 to 30 minutes to download from another system, especially from larger, older, and slower UNIX-based systems.
MobileShield™	All data is transferred real-time.
ST-ISAC	This is tracked in the interviewed organization and has been found to be very timely.
34. What has been the general estimation of the *quality* of the information that has been received?	
AIM	The quality of information has been good. This is due in part to the flexibility of AIM's reporting options. For example, the comment space is ample, and if an option is not listed in a given drop-down list, the user is able to add the desired option to the list.
DMIS	The quality of what has been received is estimated to be 95 percent.
InfraGard	The interviewed end-users agreed that the quality of information transmitted via InfraGard is excellent. The FBI has not yet had to come back and say, "Nevermind."
ITA (currently deployed prototype)	The volume of messages received to-date from the few parties using the system has been too minimal to quantify.
IRRIS	Good quality, including information from Navtec database, is guaranteed. For cargo tracking, MTMC Ops center performs weekly tests on the quality of the information received. To test

	the system, a spreadsheet query is printed and the Ops center will confirm the information with follow-up telephone calls. IRRIS is very close to 100 percent accurate. IRRIS began by using free networks, but the data received tended to be old and out-of-date. The military now purchases specific information, such as weather forecasts, to ensure the system's accuracy.
MobileShield™	All images are very clear with only slight "jerkiness" in video transmission. Voices and sounds are clear and crisp. The quality of received data is the best that the end-user interviewed expressed as ever having seen.
ST-ISAC	ST-ISAC has done a very good job. Particularly impressive was the effort to characterize items which had become public knowledge but which were inaccurate.
35. Describe the prevalent opinion of the software's available *options* for information dissemination.	
AIM	There are good options built into the system for information dissemination. Different distribution lists may be selected based on incident type. Besides email notification, cell phone text messages that the system disseminates are an effective tool as well.
DMIS	This is viewed to be acceptable. In Northern Virginia, during 9/11, the Internet was the only communication method which continued to function. The information queue function of DMIS is critical and unique. If Internet connection is lost, functionality is retained locally. When connection is restored, it starts from exactly where it left off.
InfraGard	There are not many dissemination options available. A general member does not have the ability to access as many dissemination functions as the system coordinators. Email is the main option available at this time. An individual representative from a defense contractor once supplied critical information to the coordinators of the Philadelphia chapter over a secure fax system. However, most information is exchanged via email over the VPN.
ITA (currently deployed prototype)	With the addition of an event message, this seems to be acceptable. Event message is a new feature to designate a message related to an actual incident.
IRRIS	IRRIS is always available via the Internet. It is compatible with Microsoft and most other commercial products. Users can cut and paste from IRRIS into Microsoft applications quite easily, including email, Word, Excel, and Access. IRRIS' developers based the system on the Microsoft Office format because they wanted IRRIS to interface with the most compatible software used in the world.
MobileShield™	The system allows dissemination to any unit with an IP address.

	The interviewee has been very impressed with the interoperability of the system.
ST-ISAC	This has been good and adequate. ST-ISAC will page users based on the expressed profile.
36. What is the view of the *reliability* of information dissemination that the software system has provided?	
AIM	The information dissemination is reliable.
DMIS	Anecdotally, the reliability has been quite good.
InfraGard	The interviewed end-users regard the information dissemination process as very reliable. The biggest problem is that the private workforce can be transient and changing constantly. The managers of the system at LSU may receive some undelivered emails as a result of individuals forgetting to update their information on a consistent basis. Managing the email accounts is the biggest challenge.
ITA (currently deployed prototype)	Since this is a closed system, the expectation is that the reliability should be quite good.
IRRIS	IRRIS has always worked with Microsoft programs. There have been no compatibility problems when disseminating information to customers.
MobileShield™	The information dissemination is very reliable.
ST-ISAC	This function is viewed as performing well.
37. Does the system provide for remotely notifying personnel at home or in the field?	
AIM	The system notifies remotely. When a notification is sent out, a recipient's cell phone will notify them that an AIM report has been issued. The user can then call for appropriate login information (if needed) and use the login information to access AIM from any internet terminal.
DMIS	No, this is not a current capability, and may not be a future one.
InfraGard	Not at this time. However, the coordinators have laptops that can access the Internet, and therefore, remotely display InfraGard information.
ITA (currently deployed prototype)	No, this is not yet possible.
IRRIS	Yes, right now this function is limited, but IRRIS' developers are in the process of designing more robust options. They are looking at a broad range of communication devices, as previously mentioned.
MobileShield™	The system has the capability to remotely notify personnel at home or in the field.

ST-ISAC	Yes, personnel may be notified, when out of the office, through pagers, if the numbers are provided.
38. What is the prevailing opinion of the software's available *options* for notification?	
AIM	It is felt that the available email and phone options are good.
DMIS	This is not applicable to DMIS.
InfraGard	This is not applicable to InfraGard.
ITA (currently deployed prototype)	This is not applicable to ITA.
IRRIS	The options available are quite broad, including cell phones, pagers, email, and more. The system will eventually be capable of reading text from an email directly into the telephone. The current selection is now limited for output.
MobileShield™	The options are limitless. Everyone in the entire communications chain can receive something simultaneously, or notification can be set up in tiers so only certain individuals will get a particular message.
ST-ISAC	The options for notification are thought to be adequate.
39. What has been your experience with the *reliability* of the (software) system notification methods?	
AIM	The notification methods are reliable.
DMIS	This is not applicable to DMIS.
InfraGard	This is not applicable to InfraGard.
ITA (currently deployed prototype)	This is not applicable to ITA.
IRRIS	The system notification methods are very reliable. The only necessary improvement would be to expand the range of notification topics. Currently, IRRIS will only allow for traffic incident, congestion, construction, and severe weather notifications for 27 routes in the United States. MTMC would prefer to have users key a route into the system anywhere in the world and select the various alert topics they would like to receive for that particular route. IRRIS should eventually coincide with homeland security notifications within certain spatial locations. There needs to be a broader band of notification capabilities.
MobileShield™	The system has never failed.
ST-ISAC	It has been effective in tracking down personnel at home.
40. What is the most prevalent viewpoint of the software system's effectiveness in interfacing with other software programs operated?	
AIM	AIM is relatively effective at interfacing with other software.

	Points of dissatisfaction include lacking the ability to attach a text document or a spreadsheet (any related document) to a log. Users must "paste" text from these documents directly into the log.
DMIS	The interviewed end-user thought it was good.
InfraGard	The interviewed end-users indicated that there were some initial technical difficulties installing the VPN system, but once they were able to acquire passwords and access the site, there were no problems. There are no data fields specifically designed to interface with other software programs at this time.
ITA (currently deployed prototype)	At present ITA does not interface with the interviewed organization's other software systems, since the other software resides on their own Intranet and cannot be interfaced with ITA's VPN.
IRRIS	IRRIS is highly effective in interfacing with Microsoft software programs. The basic system MTMC uses is called Intergraphs, which is an open system by GeoMedia Webmap Enterprise. They also interface with most software programs and are partners with Microsoft. Other systems may not perform these functions as well because they are not open systems.
MobileShield™	The system is flawless with any equipment that is IP based. No one has to change his or her systems to go to this technology.
ST-ISAC	There has been very limited experience with this. The secure website is accessed through an Internet browser and works well with other software. In the organization interviewed, there has not been an effort to interface secure email with any other product.
41. In what ways, if any, could these interfaces be improved?	
AIM	Allowing users to import maps and nautical charts would improve the effectiveness of AIM.
DMIS	The best way would be for other commercial entities to come on-line and write to DMIS standards. This would be particularly useful for command and control systems.
InfraGard	This is not applicable to InfraGard.
ITA (currently deployed prototype)	A VPN system stands alone. One of the interviewed end-users acknowledged the greater convenience of a system in which, for instance, email messages could be incorporated into ITA messages, or vice versa. On the other hand, there was an understanding that this would defeat the security protections in place. In the experience of at least one of the interviewed end-users, they were unable to get the floppy drive to work. They were unsure if this was due to system design or unrelated, temporary failure. While they recognize the need for security, the question

	was posed, if one had a substantial sized document or message from another source, how would one communicate it? The question was posed as "How far do you want to take security?"
IRRIS	There are no improvements necessary. IRRIS is compatible with almost any other software. Microsoft is the software industry leader. If a system is not compatible with Microsoft, no one will want it.
MobileShield™	The end-user interviewed could not think of a way in which he would want these interfaces improved.
ST-ISAC	The organization interviewed is satisfied with the current interfaces.
42. What is the most prevalent estimation of the security functions provided by the software?	
AIM	Because it is not encrypted, but is an open system using a normal Internet connection, AIM is not usable for any security level above For Official Use Only (FOUO). When CMC receives a classified document, users can post that they have received classified information but may not reveal specifics of the document over AIM.
DMIS	The interviewed end-user thought it was good. The double encryption was thought to be sufficient.
InfraGard	The process of connecting to the VPN is very good. The problem is with determining how secure the information is on the other end of the connection. InfraGard may shut down after a certain period of inactivity, but does not protect users who leave their systems vulnerable for any length of time. However, the VPN itself is very secure.
ITA (currently deployed prototype)	To the interviewed end-users, the system seems secure with the encryption provided by the VPN.
IRRIS	IRRIS maintains a high level of security. When security capability tests were conducted by the military, IRRIS received the highest rating. A login name and password are required. The password is eight characters in length. The National Security Administration (NSA) provides a template standard for the designation of letters, numbers, and symbols in an eight-character password. IRRIS follows this standard.
MobileShield™	The system meets national security encryption standards, which is a shortcoming of other security systems available.
ST-ISAC	The security provided is probably overmatched to the task. Ninety-nine percent of the information provided is not sensitive to the level of the security provided.
43. In what ways, if any, could these security functions be improved?	

AIM	CMC staff is satisfied with the level of security. If the inclusion of classified information is desired, the system can be used on a secure Internet connection.
DMIS	The interviewed end-user had no opinion on this point and acknowledged his lack of expertise in this area.
InfraGard	All of the members should belong to the VPN system. There are currently different classes of information designed for specific groups of users. It would be ideal if everyone belonged to the same system and received the same information. The problem with security across the board is not having 100 percent compliance.
ITA (currently deployed prototype)	The interviewed end-users have no suggestions at this time.
IRRIS	There are no improvements needed at this time. If MTMC knew of any improvements, this would be its number one priority.
MobileShield™	The end-user interviewed could not think of a way in which it would be desirable to improve security functions.
ST-ISAC	There is no need for improved security.
44. Have any GIS capabilities the software system possesses been used?	
AIM	CMC has made use of the GIS capabilities that the software system possesses.
DMIS	Yes, the GIS capabilities are frequently used.
InfraGard	This is not applicable to InfraGard.
ITA (currently deployed prototype)	The interviewed end-users reported that they have not yet made use of ITA's GIS capabilities.
IRRIS	Yes, all of the time.
MobileShield™	The end-user interviewed has not made use of any GIS capabilities.
ST-ISAC	This is not applicable to ST-ISAC.
45. Describe the experience with the software system's GIS capabilities.	
AIM	The provided mapping features are insufficient. Maps are basic and not helpful. CMC uses a commercial, Microsoft application (Streets & Trips) for mapping information.[28]
DMIS	Everything that has been tried has been accomplished. The interviewed organization has a great deal of real world experience in exercising.
InfraGard	This is not applicable to InfraGard.
ITA (currently deployed	This question is not applicable to the experience of the end-users interviewed.

[28] This information is reported in the interest of accuracy. Neither the National Cooperative Highway Research Program nor the McCormick Taylor Research Team endorses any product or manufacturer.

prototype)	
IRRIS	The interviewed end-user of IRRIS believes the GIS capabilities of the system are excellent. However, if one loses Internet connectivity, the capabilities of the system are lost. Therefore, IRRIS' capabilities are dependent on the quality of the Internet connection. GIS capabilities are what separate IRRIS from the rest of the world. For example, IRRIS can locate all military trucks within a 20-mile radius. The interviewed end-user is unaware of any other system that can perform a similar query over the Internet. Spatial queries are what make this system unique.
MobileShield™	This question was not applicable to the experience of the end-user interviewed.
ST-ISAC	This is not applicable to ST-ISAC.
46. Has the software system been used to conduct test simulations or drills?	
AIM	AIM was used in the TOPOFF 2 nationwide, 5-day event.
DMIS	Yes, the system has been used to conduct test simulations and drills.
InfraGard	No, the interviewed organization has not used InfraGard for the purpose of exercises or drills.
ITA (currently deployed prototype)	Yes, the system has been used to conduct test simulations and drills.
IRRIS	Yes. It has been used for numerous drills in Norfolk, VA. The Port Readiness Committee and other agencies prepared themselves to respond during exercises in which *what if* scenarios were conducted using IRRIS.
MobileShield™	The system has been used to conduct test simulations and drills.
ST-ISAC	No, the interviewed organization has not used ST-ISAC for the purpose of exercises or drills.
47. What is the prevailing view of the performance of the software system in conducting test simulations and drills?	
AIM	The system worked well. AIM has a built in feature allowing logs and incidents to be marked as *training*, allowing real events to be managed while training takes place.
DMIS	The experience has been good so far.
InfraGard	This question is not applicable to InfraGard.
ITA (currently deployed prototype)	It was only used to inform others of the participation of the interviewed organization in the TOPOFF2 exercise.
IRRIS	The quality of the system was very good in conducting simulations and drills. It performed on-the-fly rerouting to avoid major plumes and closed roads.

MobileShield™	The end-user interviewed is totally confident in the system's ability.
ST-ISAC	This question is not applicable to ST-ISAC.
48. What is the prevalent opinion of the value delivered by way of any money spent on this (software) system?	
AIM	No additional equipment has been purchased for the AIM system. The original system has lived up to its cost.
DMIS	The general comments on the system have been "That's what we wanted."
InfraGard	The value of InfraGard is good for the money, considering that the system is free of charge. The interviewed end-users feel that certain members of the InfraGard management staff at LSU are "worth their weight in gold."
ITA (currently deployed prototype)	The interviewed organization believes that it has received its money's worth.
IRRIS	For IRRIS, MTMC has spent four million dollars. This is an excellent price for a system with these extensive capabilities. IRRIS is currently competing with another system on which the military already spent half a billion dollars. The developers are asking for another half a billion dollars to fix it. The competing system is merely a tracking system, with no GIS or mapping capabilities. The developers of IRRIS have exceeded MTMC's expectations in every case. IRRIS is a nationally recognized, award-winning system.
MobileShield™	The end-user interviewed was impressed by the value of the system. The developer has put substantial R&D funds into the system and the company is confident of its value.
ST-ISAC	ST-ISAC has delivered well for the money spent. The analysis is particularly well done. Though other attractive services are offered, their additional expense has been a deterrent.

Table 5 outlines the following features and characteristics associated with these communication systems as presented in the documentation provided at the *Summit on Interoperable Communications for Public Safety*:[29]

- ❒ full name of system;
- ❒ agencies associated with systems;
- ❒ partners or sponsors;
- ❒ contacts;
- ❒ web page address;
- ❒ goals; and
- ❒ economic sectors.

Note that the questions used to develop the developer and end-user Features Matrixes were not used here because the original statement of work for this Task Order identified the systems to be surveyed and did not include these three systems.

Each of these systems is briefly described in the following narratives.

TABLE 5: FEATURES AND CHARACTERISTICS OF ADDITIONAL COMMUNICATION SYSTEMS

	GLOBAL	OASIS	RISS
FULL NAME	Global Justice Information Sharing Initiative	Organization for the Advancement of Structured Information Services	Regional Information Sharing Systems
AGENCIES	US Department of Justice (DOJ), Bureau of Justice Assistance (BJA)	A nonprofit, international consortium comprised of private industry leaders.	US Department of Justice (DOJ), Bureau of Justice Assistance (BJA)
PARTNERS OR	Partners: ❒ DOJ BJA;	OASIS has over 130 private industry	Partners: ❒ DOJ BJA;

[29] Department of Commerce, National Institute of Standards and Technology, Office of Law Enforcement Standards; Department of Justice, National Institute of Justice, AGILE Program; and Department of Homeland Security, Science and Technology Directorate, SAFECOM, *Briefing Book of Public Safety Related Groups and Programs on Interoperable Communications and Information Sharing*, Summit on Interoperable Communications for Public Safety, Office of Management and Budget, Washington, DC, June 26–27, 2003. Although this document was the primary source for the information presented here, some additional information was found on the websites associated with the systems.

	GLOBAL	OASIS	RISS
SPONSORS	❒ Office of the Special Trustee (OST); ❒ Office of Justice Programs (OJP); ❒ National Institute of Justice (NIJ); ❒ US Attorney General; ❒ International Association of Chiefs of Police (IACP); ❒ INTERPOL; ❒ FBI CJIS; ❒ National Center for State Courts; ❒ National Association for Court Management; ❒ SEARCH; and ❒ National Law Enforcement Telecommunication System (NLETS).	members that serve as system sponsors. In addition to these organizations, OASIS has a large constituency of Contributor and Individual members.	❒ Office of the Special Trustee (OST); ❒ Office of Justice Programs (OJP); ❒ National Institute of Justice (NIJ); ❒ US Attorney General; ❒ International Association of Chiefs of Police (IACP); ❒ INTERPOL; ❒ FBI CJIS; ❒ National Center for State Courts; ❒ National Association for Court Management; ❒ SEARCH; and ❒ National Law Enforcement Telecommunica-tion System (NLETS)
CONTACT(S)	Tom Henderson, Chair Information Systems Working Group (ISWG) National Center for State Courts 703-841-0200, ext. 5600 thenderson@ncsc.dni.us	Karl F. Best, Director Technical Operations Mailing: Post Office Box 455 Billerica, MA 01821 Delivery: 630 Boston Road Billerica, MA 01821 978-667-5115 f. 978-667-5114 karl.best@oasis-open.org	George March, Director RISS Office of Information Technology 610-873-9940 gmarch@risstech.riss.net

	GLOBAL	OASIS	RISS
WEB PAGE ADDRESSES	http://www.it.ojp.gov/	http://www.oasis-open.org/who/	http://www.iir.com/RISS/
GOALS	1. Promote information sharing among the justice and public-safety communities. 2. Recommend, via the US Attorney General et al., actions and approaches to facilitate effective information sharing and integration.	Develop, promote, and foster convergence and adoption of e-business standards.	Overall objective is to enhance the ability of local, state, federal, and tribal law enforcement and criminal justice agencies to identify, target, and remove criminal conspiracies and activities spanning multi-jurisdictional, multi-state, and sometimes international boundaries, and to support investigation and prosecution efforts against terrorism, narcotics trafficking, organized crime, criminal gangs, cyber crime, and violent crime.
ECONOMIC SECTORS	❒ Law enforcement ❒ Courts ❒ Public Defender ❒ Prosecution ❒ Corrections ❒ Probation/Parole	❒ Law enforcement ❒ Courts ❒ Public Defender ❒ Prosecution ❒ Corrections ❒ Probation/Parole ❒ Fire Protection ❒ Public Works ❒ Emergency Management Services (EMS) ❒ Transportation ❒ Utilities ❒ Military	❒ Law enforcement ❒ Courts ❒ Public Defender ❒ Prosecution ❒ Corrections ❒ Probation/Parole ❒ Fire Protection ❒ Public Works ❒ EMS ❒ Emergency Management ❒ Transportation ❒ Utilities ❒ Military

GLOBAL JUSTICE INFORMATION SHARING INITIATIVE (GLOBAL)

The Global Justice Information Sharing Initiative (Global) was designed to promote information sharing among the justice and public-safety communities. It is also intended that the Global network serve as an open forum for industry leaders to make recommendations for actions and approaches to facilitate effective information sharing and integration. Global aims to develop and implement a standards-based electronic information exchange capability, providing the justice community with timely, accurate, complete, and accessible information in a secure and trusted environment. The Institute for Intergovernmental Research (IIR) received a grant from the Bureau of Justice Assistance (BJA), of the US Department of Justice (DOJ), to provide coordination and management support to Global. The Global network benefits all operational justice officials.

The Global Advisory Committee (GAC) was implemented by the US Attorney General to advise the US DOJ in the establishment of the Global Initiative. The mission of the GAC is to act as the focal point for justice information systems integration activities.

The following agencies are represented on the GAC:

- ❒ Administrative Office of the US Courts;
- ❒ American Association of Motor Vehicle Administrators (AAMVA);
- ❒ American Correctional Association (ACA);
- ❒ American Probation and Parole Association (APPA);
- ❒ Conference of State Court Administrators (COSCA);
- ❒ Criminal Justice Information Services Advisory Policy Board;
- ❒ Executive Office for United States Attorneys (EOUSA);
- ❒ FBI, Criminal Justice Information Services Division (CJISD);
- ❒ International Association of Chiefs of Police (IACP);
- ❒ IACP, Division of State and Provincial Police (S&P);
- ❒ IACP, Indian Country Law Enforcement Section;
- ❒ INTERPOL, USNCB;
- ❒ Major Cities Chiefs' Association;
- ❒ National Association for Court Management (NACM);
- ❒ National Association of Attorneys General (NAAG);
- ❒ National Association of State Chief Information Officers (NASCIO);
- ❒ National Center for State Courts (NCSC);
- ❒ National Conference of State Legislatures (NCSL);
- ❒ National Congress of American Indians (NCAI);
- ❒ National Council of Juvenile and Family Court Judges (NCJFCJ);
- ❒ National Criminal Justice Association (NCJA);
- ❒ National District Attorneys Association (NDAA);
- ❒ National Governors Association (NGA);
- ❒ National Law Enforcement Telecommunication System (NLETS);
- ❒ National Legal Aid and Defender Association (NLADA);
- ❒ National Sheriffs' Association;
- ❒ SEARCH, the National Consortium for Justice Information and Statistics;
- ❒ US Department of Homeland Security (DHS);

- ❒ US DOJ, Justice Management Division;
- ❒ US Department of the Treasury; and
- ❒ US Drug Enforcement Administration.

GAC has concentrated its expertise on the challenges and opportunities surrounding justice and public safety communication. During 2002, GAC successfully completed the following actions to promote the secure exchange of information while safeguarding citizens' constitutional rights:

- ❒ facilitated a Web-based standards registry program, promoting national systems interoperability;
- ❒ facilitated an ongoing Justice Extensible Markup Language (XML) Data Project, yielding—
  - ○ reconciliation between disparate XML specifications, enhancing justice information sharing among the courts, local police, the transportation community, and federal law enforcement,
  - ○ production of a Justice XML Data Dictionary containing hundreds of common data elements,
  - ○ evolution of the Justice XML Data Dictionary effort toward more universal applicability by using the latest information sharing protocols, and
  - ○ collaboration with the XML.GOV project to determine how Global XML efforts can serve as a model for XML registries;
- ❒ explored ways in which Global can interface with and support the Office of Homeland Security (OHS) information sharing mission;
- ❒ formed a new working group to examine intelligence information[30] sharing;
- ❒ supported the drafting of *Global Guidelines for Securely Sharing Justice and Law Enforcement Information*;
- ❒ expanded membership, to represent the changing face of justice-involved agencies; and
- ❒ developed a unique commodity: trust.[31]

Building on these achievements, next steps for Global include promoting the coordination of related standards via population and use of the Justice Standards Registry for Information Sharing, exploring the applicability of Enterprise Architecture to facilitate broad scale information sharing, confirming safeguards against misuse of personal information and improving criminal records reliability, promoting acceptable integrated justice system security measures, and, as the landscape of justice-interested agencies broadens to meet new challenges to the nation, informing and collaborating with all parts of the justice and public safety communities involved in information sharing activities.

---

[30] Refers to secure, but unclassified, information.

[31] This is, perhaps, the Committee's most important accomplishment. Through time and effort GAC has engendered an *espirit de corps* among members from disparate constituencies and levels of government, resulting in a willingness to reconcile proprietary issues in pursuit of the common goal of sharing information.

Mission and Guiding Principles of GAC

GAC's mission is to improve the administration of justice and protect the nation's public by promoting practices and technologies for the secure sharing of justice-related information.

GAC operates under the auspices of BJA, OJP, US DOJ, and advises the federal government, specifically through the Assistant Attorney General, OJP, and the US Attorney General, in facilitating standards-based electronic information exchange throughout the justice and public safety communities. The broad scope of the effort is fundamental, because public and practitioner safety is best secured when all players, from patrol officers to prosecutors and from courts officials to corrections personnel, have access to timely and accurate information.

Guiding principles of GAC are as follows.

- ❒ Bring together representatives from the entire justice community and related entities, including private industry, to overcome the barriers to justice information sharing across agencies, disciplines, and levels of government.
- ❒ Promote the development and implementation of standards that facilitate seamless exchange of information among justice and related systems.
- ❒ Provide information that supports sound business decisions for the planning, design, and procurement of cost-effective, interoperable information systems.
- ❒ Promote constitutional values and individual rights by ensuring the accuracy and security of justice information, and the implementation of appropriate privacy safeguards.
- ❒ Recommend concepts that leverage existing infrastructure, capabilities, and functionality.

GAC operates in accordance with Federal Advisory Committee Act (FACA) provisions and convenes twice a year in Washington, DC. Meetings are announced in the *Federal Register*, and the public is welcome as observers.

In the fall of 2002, per FACA term guidelines, the US Attorney General reviewed and reauthorized the Global Initiative for a succeeding two-year term. As part of this reauthorization, the project underwent a name change from the *Global Justice Information Network* to the *Global Justice Information Sharing Initiative*. This was done to more adequately represent the project's goal.

Leadership

GAC leadership is normally elected every two years. However, in early 2002, midway through the regular term, Colonel Michael D. Robinson resigned as Director of the Michigan State Police to assume a command position within the Transportation Security Administration (TSA); he also resigned as GAC Chair and as the representative of the IACP. Consequently, per GAC bylaws, the Vice Chair moved to the position of Chair, and committee members elected a new Vice Chair. Elections resumed their normal cycle in the spring of 2003.

The GAC Executive Steering Committee (ESC) consists of the GAC Chair and Vice Chair, the working group Chairs, and two at-large GAC representatives. The two at-large representatives are nominated and elected by the ESC. ESC has five major responsibilities.

- ❒ Set priorities, direct research, and prepare advisory recommendations for the approval of GAC and, upon its approval, forward advisory recommendations to the Assistant Attorney General, OJP, and the US Attorney General (or the designated appointee of the US Attorney General).
- ❒ Schedule meetings and develop GAC meeting agendas with the final approval of GAC Chair and the designated federal official.
- ❒ Consolidate and report GAC recommendations to other appropriate organizations, as necessary.
- ❒ Track and report results and/or actions taken on GAC concerns and recommendations.
- ❒ Solicit additional technical, professional, and administrative assistance to effectively and adequately address GAC concerns and support GAC activities.

Working Groups

GAC working groups, comprised of committee members and other subject-matter experts, expand the GAC's knowledge and experience. These groups are formed around timely issues impacting justice information sharing and meet as often as necessary. During 2002, the following working groups supported GAC:

- ❒ Infrastructure/Standards;
- ❒ Privacy/Information Quality;
- ❒ Security; and
- ❒ Outreach.[32]

Institute for Intergovernmental Research (IRR)

Global is a project designed by the Institute for Intergovernmental Research (IIR), a Florida-based nonprofit research and training organization that specializes in law enforcement, juvenile justice, and criminal justice issues. IIR provides local, state, and federal law enforcement agencies with tools to promote greater governmental effectiveness. It is specifically organized to conduct non-partisan research and management studies regarding the role and function of the branches and agencies of these government bodies. IRR provides policy research and technical training regarding the assessment of operational, management, and administrative systems within the government. The Regional Information Sharing System (RISS) is also a project produced by IIR. The characteristics of RISS are briefly presented in an upcoming subsection.

[32] Primary source for GAC information is the *Global Justice Information Network Annual Report 2002* at http://www.it.ojp.gov/global/outreach/37/global_report_2002.doc.

In summary, Global is a group of groups, representing more than thirty independent organizations spanning the spectrum of law enforcement, judicial, correctional, and related bodies. Member organizations participate in Global out of shared responsibility and shared belief that, together, they can bring about positive change in inter-organizational communication and data sharing. More information regarding the Global Sharing Initiative can be found at http://www.it.ojp.gov/.

ORGANIZATION FOR THE ADVANCEMENT OF STRUCTURED INFORMATION SERVICES (OASIS)

The Organization for the Advancement of Structured Information Services (OASIS) is an international consortium with headquarters in North America and representation in Europe. It is a nonprofit organization dedicated to accelerating the adoption of product-independent formats based on public standards. These standards include SGML, XML, HTML, as well as others related to structured information processing. Members of OASIS are providers, users, and specialists of the technologies that make structured information standards work in practice. Collectively, OASIS represents those with a vested interest in XML, SGML, and other structured information standards.

OASIS provides an open forum for members to discuss market needs and directions and recommend guidelines for product interoperability. The consortium creates, receives, coordinates, and disseminates information describing methodologies, technologies, and implementations of the standards. OASIS claims it is not another standards body. Its work complements standards bodies, focusing on making these standards easy to adopt and the products practical to use in real world open system applications. Where appropriate, OASIS recommends specific application strategies over others as ways in which various products can better provide interoperability for users. OASIS helps to apply structured information standards, not create more.

OASIS is financially supported by those benefiting most from its activities: (1) the software and service providers who want market growth and (2) customers who prefer to receive information and are offered an open forum in which to address the vendor community as a whole. Any company, organization, or individual who would benefit by representation in the consortium is eligible for membership.

Many members of OASIS are heavily involved with national, international, and industry-wide standards activity. OASIS does not replace that activity, but embraces it while seeking to achieve industry consensus in support of it with the help of its technical liaisons.

OASIS Membership

The logos of OASIS sponsors are featured on the OASIS home page and in the OASIS booth at conferences. Only sponsors can be quoted or mentioned in OASIS press releases and listed on Consortium Data Sheets. See http://www.oasis-open.org/join/benefits.shtml for more information.

Individuals may also participate in any and all OASIS technical committees, but without voting rights and promotional benefits.

Organizations or individuals considering OASIS membership should review the OASIS bylaws, Intellectual Property Rights Policy and Technical Committee Policy. These documents provide valuable insight into how the consortium operates and details the rights and requirements of members.

An OASIS Member Section (MS) is an established group of consortium members who share a common interest in an industry or technology. OASIS' MS is governed by its own steering committees, which report to the OASIS Board of Directors. Current OASIS MSs include Auto Repair, CGM Open, LegalXML, Public Key Infrastructure (PKI), and Universal Description, Discovery, and Integration (UDDI). Affiliation with an OASIS MS is completely optional. All members of OASIS are eligible to participate in all technical committees without restriction. Every organization that joins OASIS has the option to designate support for one or more OASIS MSs.

OASIS does not impose any time or resource commitments on consortium membership. Members' abilities to contribute to OASIS technical work vary greatly over time and among organizations.

OASIS hosts several general member meetings each year in order to communicate information of interest to the entire consortium, encourage networking between members, and facilitate collaboration between technical committees. Attendance at these general member meetings is beneficial, but not mandatory. OASIS technical committee work is accomplished via email, teleconference, and/or face-to-face meetings.

If one is interested in developing an XML specification within an open process, joining OASIS is the first step. Any group of three or more OASIS members can form a technical committee to standardize virtually anything related to the interoperability of structured information systems. OASIS serves as a home for industry groups and trading communities interested in developing standards. Advancing a technical agenda within OASIS expands participation to an internally recognized group of standards experts and users in the public and private sectors.

OASIS Membership Categories and Cost

OASIS offers three categories of membership: sponsor, contributor, and individual. All categories take advantage of exclusive OASIS membership benefits. Each category is described below in terms of costs and benefits.

Sponsor

Sponsors pay $13,500.00 USD per year for membership in OASIS. In addition to technical participation, OASIS sponsor membership provides organizations with the highest level of promotional benefits, including:

TABLE 6: COST FOR OASIS CONTRIBUTOR MEMBERSHIP BY COMPANY SIZE AND TYPE

COMPANY SIZE OR TYPE[33]	CONTRIBUTOR MEMBERSHIP COST (USD per year)
Ten or more employees	$5,750.00
Less then ten employees	$2,750.00
Non-profit organization	$1,000.00

- ❒ company logo featured on OASIS homepage;
- ❒ link from OASIS website to company site;
- ❒ company logo displayed in the OASIS exhibit booth;
- ❒ company name featured on OASIS press releases;
- ❒ company logo featured in OASIS presentation materials;
- ❒ company press releases featured on XML.org homepage and included in the XML.org Daily News, delivered to more than 5,000 subscribers;
- ❒ use of OASIS logo on company marketing materials; and
- ❒ unlimited distribution of company news to OASIS members-only email list.

Contributor

The cost for a contributor membership is dependent upon the size of the company. Table 6 illustrates the breakdown of an OASIS contributor membership for each company.

Benefits include:

- ❒ OASIS logo on company marketing materials;
- ❒ OASIS member logo on website;
- ❒ OASIS member logo in tradeshow booth.

Individual

An individual OASIS membership costs $250.00 USD per year. OASIS offers Individual memberships to those without corporate affiliation who wish to contribute to the advancement of interoperability standards. The OASIS individual member program is intended primarily for those involved in academia. Benefits are exclusive to the named individual, who may participate fully in all OASIS technical committees and consortium meetings. Companies are not eligible for individual membership, and employers of

[33] The number of employees refers to the number of employees in the contributor company. To qualify for the non-profit category, the applicant must be a legally recognized non-profit organization, university, or local or state government agency or a federal agency of a non-G-10 country.

Individual members do not receive recognition, voting rights, or technical/promotional benefits from OASIS.

REGIONAL INFORMATION SHARING SYSTEMS (RISS)

To facilitate the sharing and exchange of critical information, the Regional Information Sharing Systems (RISS) operates the RISS Secure Intranet (*riss.net*), a nationwide sensitive, but unclassified (SBU) secure communications and information sharing network for local, state, federal, and tribal law enforcement and criminal justice member agencies. RISS operates the only secure Web-based nationwide network for communication and exchange of criminal intelligence.

With establishment of the RISS Anti-Terrorism Information Exchange (RISS ATIX) Program, RISS expanded accessibility to *riss.net* to deliver secure inter-agency communication, information sharing, and dissemination of national security, disaster, and terrorist threat information to an additional group of users. Individuals, referred to as RISS ATIX participants, include executives and officials from government and non-government communities with responsibility for planning and implementing prevention, response, mitigation, and recovery efforts regarding terrorism and disasters. As appropriate to their roles and responsibilities within and among their affiliated communities, RISS ATX participants are provided access to specific resources available via *riss.net*. RISS ATX communities are those government and non-government organizational entities whose executives and officials are responsible for planning and implementing prevention, response, mitigation, and recovery efforts regarding terrorism and disasters.

RISS resources available electronically via *riss.net* include:

- ❒ RISS Criminal Intelligence Database Pointer Systems (RISSIntel & RISSNET II);
- ❒ RISS Investigative Leads Bulletin Board (RISSLeads);
- ❒ RISS National Gang Database (RISSGang);
- ❒ Electronic linking to node partner systems and other information resources;
- ❒ RISSSearch;
- ❒ RISSTraining;
- ❒ TechPage; and
- ❒ secure email.

RISS ATIX resources include:

- ❒ RISS ATIX Bulletin Board;
- ❒ RISS ATIX website, with individual community web pages; and
- ❒ secure email.

RISS has a number of ongoing initiatives and continues to research technologies and information sharing concepts that would enhance and augment the capabilities and resources provided via the *riss.net* infrastructure. Research and development are continuing in the areas of:

- ❒ offline notification of time sensitive alerts and information;
- ❒ use of secure instant messaging in the RISS environment;
- ❒ expansion of secure chat features in the RISS environment; and
- ❒ development of secure Web conferencing with whiteboard functionality.

Additionally, RISS continues to develop relationships with other SBU systems in order to enhance and expand the ability to share sensitive and timely information in a secure manner.

RISS provides technology resources and the *riss.net* infrastructure to enable the integration and electronic connection of member agency law enforcement information technology systems as nodes on *riss.net*. RISS node partners include the High Intensity Drug Trafficking Area (HIDTA) Investigative Support Centers, the Southwest Boarder States Anti-Drug Information System (SWBSADIS), the El Paso Intelligence Center (EPIC) Clandestine Laboratory Seizure System (CLSS), and a number of state law enforcement information technology systems.

Riss.net is the secure infrastructure providing the communications backbone for implementation of the Multistate Anti-Terrorism Information Exchange (MATRIX) project. MATRIX's goal is to increase and enhance the exchange of sensitive terrorism information and other criminal activity information among local, state, and federal agencies. The project leverages and integrates existing and proven technology to provide a new capability to assist law enforcement in identifying and analyzing terrorist and other criminal activity, and appropriately disseminating information to law enforcement agencies nationwide in a secure, efficient, and timely manner. MATRIX has the following three primary objectives.

1. Use factual data analysis from existing data sources and data integration technology to improve the usefulness of information contained in multiple types of document storage systems.

2. Provide a mechanism to become nodes on *riss.net* for electronic information exchange among participating agencies.

3. Encourage the exchange of information via secure state websites.

RISS is composed of six regional centers that share intelligence and coordinate efforts against criminal networks operating in many locations across jurisdictional lines. These RISS Intelligence Centers provide a number of services to member agencies, including:

- ❒ information sharing;
- ❒ telecommunications services;
- ❒ analytical and intelligence services;
- ❒ investigative support;
- ❒ confidential funds;
- ❒ specialized equipment;
- ❒ specialized training; and
- ❒ publications and bulletins.

Typical targets of RISS activities are drug trafficking, terrorism, violent crime, cybercrime, gang activity, and organized criminal activities. Each center, however, selects its own target crimes and the range of services provided to member agencies. There are six regional RISS centers:

- ❒ Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network (MAGLOCLEN), includes Delaware, Indiana, Maryland, Michigan, New Jersey, New York, Ohio, Pennsylvania, DC, and some member agencies in England, Ontario, Quebec, and Australia;
- ❒ Mid-States Organized Crime Information Center (MOCIC), includes Illinois, Iowa, Kansas, Minnesota, Missouri, Nebraska, North Dakota, South Dakota, Wisconsin, and some member agencies in Canada;
- ❒ New England State Police Information Network (NESPIN), includes Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, Vermont, and some member agencies in Canada;
- ❒ Regional Organized Crime Information Center (ROCIC), includes Alabama, Arkansas, Florida, Georgia, Kentucky, Louisiana, Mississippi, North Carolina, Oklahoma, South Carolina, Tennessee, Texas, Virginia, West Virginia, Puerto Rico, and the US Virgin Islands;
- ❒ Rocky Mountain Information Network (RMIN), includes Arizona, Colorado, Idaho, Montana, Nevada, New Mexico, Utah, Wyoming, and some member agencies in Canada; and
- ❒ Western States Information Network (WSIN), includes Alaska, California, Hawaii, Oregon, Washington, and some member agencies in Canada, Australia, and Guam.

Figure 8 illustrates the quantity of member agencies in each of the six regional RISS Intelligence Centers.

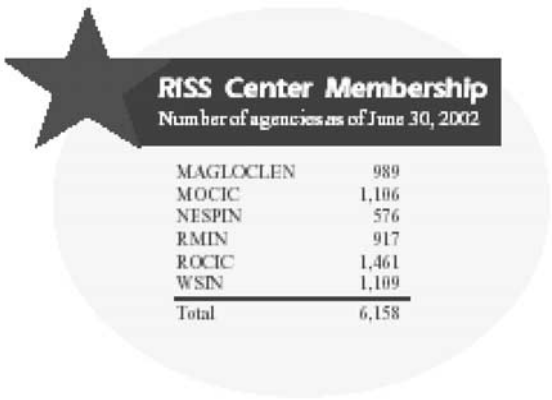


FIGURE 8: QUANTITY OF MEMBER AGENCIES PER EACH RISS CENTER[34]

[34] Image reproduced from Institute for Intergovernmental Research, Regional Information Sharing Systems Program, *The RISS Program: 2001, Membership and Service Activity,* Tallahassee, Florida, July 2002, http://www.iir.com/Publications/RissProgram2001.pdf.

Each RISS center must comply with US DOJ Program Guidelines and 28 CFR Part 23, Criminal Intelligence Systems Operating Policies. RISS serves over 6,400 member law enforcement agencies in 50 states, Canada, the District of Columbia, Australia, Guam, the US Virgin Islands, England, and Puerto Rico. Each RISS center has from 599 to over 1,550 member agencies. The vast majority of member agencies are at the municipal and county levels, but almost 400 state agencies and over 840 federal agencies are also members. The Drug Enforcement Administration (DEA), Federal Bureau of Investigation (FBI), US Attorney's Offices, Internal Revenue Service (IRS), Secret Service, Customs, and the Bureau of Alcohol, Tobacco, Firearms, and Explosives are among the federal agencies participating in the RISS program.

Highlights of RISS Services

RISS is federally funded by DOJ-BJA and is produced by the Institute for Intergovernmental Research (IIR). RISS services currently available to member law enforcement and criminal justice agencies are briefly described below.

- ❒ Information sharing and communication network, including:
  - access to timely computerized information on criminal suspects and activities;
  - secure intranet for electronic networking of law enforcement agencies throughout the US;
  - electronic linking of the six RISS center criminal intelligence databases via *riss.net*; and
  - electronic linking to other systems, such as the Southwest Border States Anti-Drug Information System Network, High Intensity Drug Trafficking Areas, and other state intelligence systems.

- ❒ Analysis of multi-jurisdictional crime, including:
  - analysis of complex case data connecting subjects and criminal events;
  - analysis of linked RISS databases to identify major criminal conspiracies; and
  - information surveys and analysis of gangs, firearms, trafficking, and violent criminal activities to assist member law enforcement agencies.

- ❒ Information sharing conferences with specialized training, such as:
  - National Conference on Serial Murder;
  - regional conferences on cybercrime, terrorism, gang activity, firearms trafficking, and violent criminal activity;
  - regional conferences on methamphetamine labs; and
  - training to build member agency expertise in investigative techniques, violent crime initiatives, and emerging crime problems.

- ❒ Loan of sophisticated investigative equipment not otherwise available or too costly for one agency.

- ❒ Funds for purchase of evidence, information, or other investigative expenses to support multi-jurisdictional investigations.

RISS Space Available for ISACS

At the NIST *Summit on Interoperable Communications for Public Safety o*n June 26–27, 2003, RISS representatives indicated that a new facility was being acquired to increase the effectiveness of its operations. They also stated that, within this larger facility, there should be enough space to house one or more Information Sharing and Analysis Center (ISAC) operations as well.[35] RISS representatives are showcasing the system's ability to link with other intelligence systems that share a common goal of secure information exchange among key industry leaders.

[35] The NCHRP Senior Program Officer (SPO), Stephan Parker, relayed this information to McCormick Taylor's John N. Balog on July 11, 2003.

IMPLEMENTATION OPTIONS ASSOCIATED WITH THE ESTABLISHMENT OF AN AASHTO HIGHWAY TRANSPORTATION ISAC

This section entails a comprehensive investigation of the phenomenon of Information Sharing and Analysis Centers (ISACs), with a focus on their applicability for the highway transportation industry. This review comprises the following subsections:

- ❒ Information Sharing and Analysis Centers: An Overview;
- ❒ Information Sharing and Analysis Centers for the Highway Sector: An Assessment of Costs; and
- ❒ Information Sharing and Analysis Centers for the Highway Sector: Characteristics of ISAC Formulation and Operation for the Highway Sector.

These three subsections have been designed to present a variety of issues that are important to this decision-making process. The first subsection addresses the concepts of ISACs and how they are being utilized by other critical infrastructure sectors within the US economy. The second and third subsection of this chapter respectively consider the costs associated with the implementation of an ISAC, and the organizational characteristics of an ISAC.

INFORMATION SHARING AND ANALYSIS CENTERS: AN OVERVIEW

The American Association of State Highway and Transportation Officials (AASHTO) is in the process of establishing the approach it will be taking regarding the potential implementation of an Information Sharing and Analysis Center (ISAC) for the critical infrastructure associated with the highway transportation sector within the United States.

WHAT IS AN ISAC?

It is a comparatively recent innovation on the part of many critical infrastructure industries in the US to cooperate on security matters by means of an ISAC.

An ISAC is a means for the members of a critical infrastructure sector within the US economy (e.g., electric utility suppliers, water distributors, or financial institutions) to share specific industry information, resources, and information regarding security within their sector, in a relatively secure manner. There are a number of different models for how ISACs work and are structured, but the common theme represents a partnership between government and the critical infrastructure industry to address security concerns. In private sector models, the concept of anonymity may be considered quite important, so that security breaches of which a particular company may be aware do not immediately find their way into the media. This is particularly important to the cyber industry via the information technology ISAC (IT-ISAC). This concern for maintaining the developed information as private to the members of the economic sector extends to many of the other functional areas as well.

In addition, the more formalized ISACs, often formed as limited liability corporations (LLCs) with boards of directors, provide a means to communicate information at a metaphorical distance from government regulators as well as the corporations they were created to serve.

ISAC History

Two United States Presidential Directives are responsible for the current state of ISACs. These are Presidential Decision Directive 63 (PDD-63) and Executive Order 13231.

Presidential Decision Directive 63

PDD-63, created under President Clinton in 1998, was the original impetus for ISACs. The directive grew from a report in October 1997 written by the President's Commission on Critical Infrastructure Protection entitled *Critical Foundations: Protecting America's Infrastructures* (Critical Foundations). The Commission's work was spurred as a result of a few, highly publicized, but not particularly destructive, computer viruses that alarmed the general public and demonstrated how vulnerable ordinary computers, used in business and for personal use, are to a cyber attack. The publicity surrounding the *Michelangelo* virus in 1992 and the *Satan Bug* virus in 1993, which was written by a minor, demonstrated how easily destructive codes could be written and how vulnerable ordinary users had become. While these viruses were MS-DOS-based, a new generation of viruses had also penetrated the Windows 95 platform.[1]

The very physical terrorist acts of the World Trade Center bombing in February 1993 and the Oklahoma City bombing in April 1995 also colored the Commission's work. In addition, much attention was focused at that time on the impending and well-publicized Y2K situation and the dire consequences predicted by some prognosticators. The Commission realized that, as many industries relied increasingly on the power of new technology, the Internet, and growing automatization and the power of computers to operate and control vital functions, cyber threats, when implemented, could prove to be destructive to the function of numerous critical industries. While the issue of physical threats was certainly addressed to a degree in both the Commission's work and the subsequent PDD-63, it is safe to say that in a pre-September 11th, 2001 environment, the issue of cyber threats was the predominant concern.

Critical Industries

In Critical Foundations, eight key industries were considered to be particularly central to the wellness of the nation's economy and social order. These were:

[1] The mention of specific operating systems is made here to be factually correct. The National Cooperative Highway Research Program, Transportation Research Board and McCormick Taylor Research Team do not endorse any product, service, or developer.

- ❒ information and communications;
- ❒ electric power;
- ❒ gas and oil production and storage;
- ❒ banking and finance;
- ❒ transportation;
- ❒ water supply;
- ❒ emergency services; and
- ❒ government services.

By the time of PDD-63's issuance, this list had been refined and expanded somewhat to include the above-mentioned industries as well as subsets of some sectors. For instance, the transportation industry was regarded as containing:

- ❒ aviation;
- ❒ highways, including the trucking and intelligent transportation systems (ITS) sectors;
- ❒ public transportation;
- ❒ pipelines;
- ❒ rail; and
- ❒ water-based shipping.

Emergency services were expanded to include:

- ❒ emergency law enforcement services;
- ❒ emergency fire service;
- ❒ continuity of government services; and
- ❒ public health services including prevention, surveillance, personal health services, and laboratory services.

Government Agency Liaison

PDD-63 also identified the roles for certain federal government departments and agencies in providing liaisons to each of the identified sectors. These are shown in Table 7.

In addition, certain agencies were assigned responsibility for special functions related to the directive, as shown in Table 8.

National Infrastructure Protection Center (NIPC)

The National Infrastructure Protection Center (NIPC) was another construct suggested within PDD-63. NIPC, directed by PDD-63 to be created by the FBI, was designed to serve as *a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity*.[2] The intent was to create this new group

[2] The White House, *Presidential Decision Directive 63*, Washington, DC, May 22, 1998.

TABLE 7: CRITICAL INDUSTRY SECTORS FROM PDD-63 AND AGENCY LIAISONS

INDUSTRY SECTOR	LEAD FEDERAL DEPARTMENT OR AGENCY
Information and communications	Commerce
Banking and finance	Treasury
Water Supply	Environmental Protection Agency (EPA)
Transportation: ❒ aviation; ❒ highways, including trucking and intelligent transportation systems (ITS); ❒ public transportation; ❒ pipelines; ❒ rail; and ❒ water-based shipping.	Transportation
Emergency law enforcement services	Justice, Federal Bureau of Investigation (FBI)
Emergency fire service	Federal Emergency Management Agency (FEMA)
Continuity of government services	FEMA
Public health services including: ❒ prevention; ❒ surveillance, ❒ personal health services; and ❒ laboratory services.	Health and Human Services (HHS)
Electric power	Energy
Oil and natural gas production and storage	Energy

TABLE 8: SPECIAL FUNCTION ASSIGNED FROM PDD-63 AND AGENCY LIAISONS

INDUSTRY SECTOR	LEAD FEDERAL DEPARTMENT OR AGENCY
Law enforcement and internal security	Justice, FBI
Foreign intelligence	Central Intelligence Agency (CIA)
Foreign affairs	State
National defense	Defense

from professionals knowledgeable about computer crimes and infrastructure protection, drawn from the FBI, the United States Secret Service (USSS), and other entities from the Department of Defense (DOD), the intelligence community, and other agencies.

While lacking the title of formal coordinator of ISAC activity, NIPC became responsible for much of the effort to assist and track the formation of ISACs. PDD-63 specifically called for the cooperation of all executive departments with the efforts of NIPC. Furthermore, NIPC was intended to be an information middleman if other agencies learned of threats and warnings as well as actual attacks on critical governmental or industrial infrastructure. NIPC was empowered by PDD-63 to sanitize law enforcement and intelligence information for subsequent distribution in the form of analyses and reports to federal, state, and local agencies, as well as to the owners of critical infrastructures and to associated ISACs. NIPC was also authorized to issue attack warnings or alerts regarding increases in threat conditions to ISACs or critical infrastructure owners. In short, NIPC was intended to be the national focal point for the gathering of threat information regarding critical infrastructure. NIPC also had major responsibilities in the event of an actual attack to assist DOD or the intelligence community in facilitating and coordinating an appropriate response.

The Envisioned Role of the ISAC

The role of an ISAC is to represent a critical infrastructure industry in the area of security, accepting information from a variety of sources and transferring it to the government, through NIPC and on to other government sources, and then back to its members in the form of corroborated intelligence. This concept is graphically depicted in Figure 9. Figure 9 is illustrative in the sense that the individual members of the ISACs, though connected to each other through the ISAC, are not directly connected to each other. This is an intentional structure. In many industries, characterized by private corporations, members are in competition with each other. To be in direct contact might raise anti-trust issues. While these members may be willing to cooperate with each other to a degree in the area of collective security, that cooperation may not extend a great deal beyond this issue. The ISAC is, in many cases, operated as an independent, private corporation that prefers an arms-length relationship with its members. This is important from a liability perspective as well as in creating a separate venue in which cooperation, rather than competition, is the desired outcome. Additionally, in certain industries, the closest government counterpart with expertise in a particular field has a regulatory function. Private corporation members of certain ISACs do not usually favor the concept of closer ties with the government agency empowered to regulate their behavior.

From the government's perspective, attributable information is the most useful, but non-attributable data is far better than no information at all. If receiving information from the field via the ISAC is a method by which critical infrastructure sectors feel comfortable, then it is far better to receive information in a form those sectors can accommodate. Most importantly, for both industry and the government, more is better. The more comfortable individual entities feel about joining an ISAC, the more likely they will feel comfortable about sharing information and broadly disseminating warnings, alerts, and best practices.

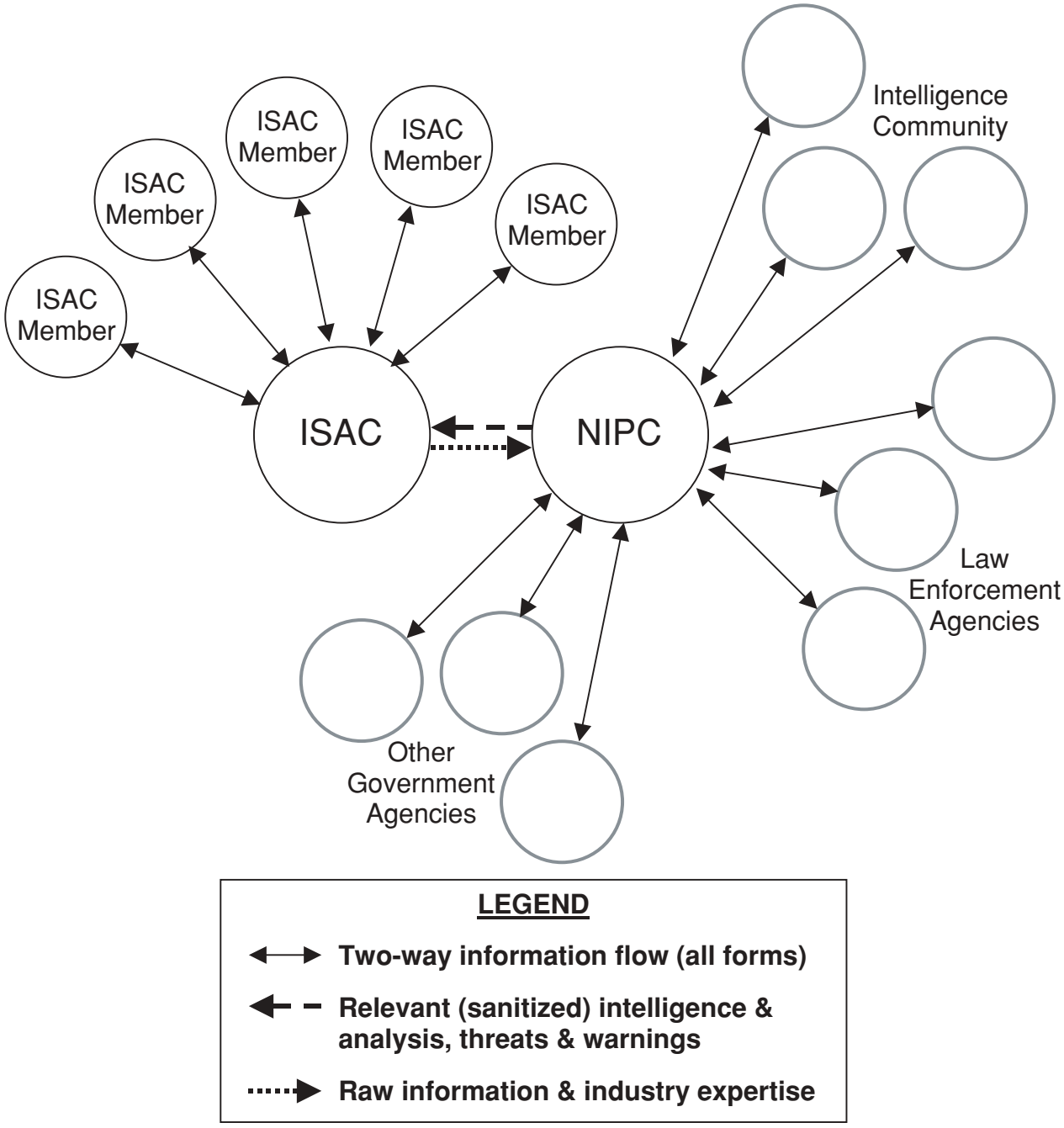


FIGURE 9: THE ISAC CONCEPT

From both government and private sector perspectives, having many members may translate into more data points upon which to base the analysis of anomalous events. This assists everyone involved as it serves both the interests of government and industry and encourages them to share information in a way that incidents can, at best, be prevented and, at least, be anticipated, so that industry experts are better able to prepare an appropriate response.

Private-Public Partnership Guidelines

PDD-63 also spelled out certain guidelines to be used in this new effort to establish private-public partnerships. Among these were:

- ❒ partnerships should emphasize protecting critical infrastructures as a shared responsibility of private owners/operators and the government;
- ❒ partnerships should realize that frequent reassessment is necessary to adapt to changing technology, vulnerabilities, and the threat environment;
- ❒ critical infrastructure protection should ideally be market-driven and voluntary, rather than regulatory, and regulation should only be used as a last resort *in the face of a material failure of the market to protect the health, safety and well being of the American people*;[3]
- ❒ agencies should not be prevented from trying to harness economic incentives (as indeed some have), assisting private owners and operators in attaining and maintaining the highest possible levels of security;
- ❒ the *full authorities, capabilities and resources of the government, including law enforcement, regulation, foreign intelligence and defense preparedness* should be brought appropriately to bear on the problem of critical infrastructure protection;
- ❒ privacy rights should be respected and consumers and operators should have an expectation that received information would be treated confidentially, with accuracy and reliability;
- ❒ the federal government should, in its research, development, and procurement, advance the efforts of finding the best possible means for infrastructure protection;
- ❒ the federal government should serve as a model of how infrastructure protection should be effected and should distribute this knowledge, whenever possible;
- ❒ focusing on prevention as well as threat and crisis management, private sector owners and operators should be encouraged to provide the government with information necessary to assist officials in protecting critical infrastructure to the maximum extent feasible; and
- ❒ cooperation, coordination, and consideration of the needs of first responders, as well as state and local governments, should be included as part of any critical infrastructure protection planning.

Executive Order 13231

Executive Order 13231 (E.O. 13231), issued by President George W. Bush on October 16, 2001, reiterated many of the goals and commitments of PDD-63. It also focused heavily on cyber threats to the nation's critical infrastructures. Of principal note, as the issuance of E.O. 13231 came only weeks after September 11, is its emphasis on emergency preparedness communication.

The Order established a new executive level board, entitled the President's Critical Infrastructure Protection Board, and focused on the duties, responsibilities, and relationship

[3] Ibid.

of the new board with other relevant governmental entities regarding critical infrastructure protection. Among its responsibilities was information sharing with the critical industries, state and local governments, and non-governmental entities to ensure that systems are in place to share threat warning, analysis, and recovery information with government operations centers, ISACs, and other related operations centers.[4]

E.O. 13231 also established the National Infrastructure Advisory Council (NIAC), a group composed of senior executives in critical infrastructure corporations, as well as representatives from academia and state and local governments. One major function of the Council was to monitor the development of ISACs and make recommendations on how cooperation among ISACs, NIPC, and other governmental entities can best be fostered.[5]

Identified Working ISACs

As suggested in Presidential Decision Directive 63 (PDD-63), the following industry sectors have formed ISACs:

- ❒ Information Technology;
- ❒ Telecommunications;
- ❒ Banking and Finance;
- ❒ Water Supply;
- ❒ Trucking (originally envisioned as part of Highways);
- ❒ Mass Transit and Railroads (Surface Transportation);
- ❒ Emergency Law Enforcement Services;
- ❒ Emergency Fire Service;
- ❒ Continuity of Government Services;
- ❒ Electric Power; and
- ❒ Energy (Oil and Natural Gas Production and Storage).

The following sector ISACs have been established as well, though not specifically identified in the Directive:

- ❒ Food;
- ❒ Chemicals; and
- ❒ Interstate.

Table 9 outlines the critical infrastructure ISACs identified by PDD-63 that are currently in operation along with important attribute information.[6]

---

[4] The White House, President George W. Bush, *Executive Order 13231: Critical Infrastructure Protection in the Information Age*, Washington, DC, October 16, 2001.

[5] Ibid.

[6] Some materials in Table 9 are reproduced from: Center for Infectious Disease Research & Policy, *Critical Infrastructure ISACs*, University of Minnesota, August 2002, http://www.cidrap.umn.edu/cidrap/files/20/table-isacs.pdf. However, Table 9 has been updated to include information regarding ISACs through July 2003.

TABLE 9: OUTLINE OF ISACS CURRENTLY IN OPERATION

SECTOR	ACRONYM	WEB INFO	START DATE	AGENCY (PDD-63)	SECTOR COORDINATOR	DEVELOPER
Information Technology	IT-ISAC	www.it-isac.org	01/01	Department of Commerce, National Telecommunications & Information Administration (NTIA)	Information Technology Association of America (ITAA)	ITAA
Telecommu-nications	NCC-ISAC	www.ncs.gov/ncc	01/00	Department of Commerce	National Coordinating Center for Telecommu-nications (NCC)	NCC
Financial Services	FS-ISAC	www.fsisac.com	10/99	Department of Treasury	Citigroup, Chief Information Security Officer	
Water Supply	Water ISAC	www.waterisac.org	12/02	Environmental Protection Agency (EPA) Water Protection Task Force	Association of Metropolitan Water Agencies (AMWA)	EMWA, $600,000 EPA grant
Trucking	Trucking ISAC	www.truckline.com/insideata/isac	03	US DOT	American Trucking Associations (ATA)	ATA, US DOT
Surface Transportation (Railroads)	ST-ISAC	www.surfacetransportationisac.org	10/01	US DOT	Association of American Railroads (AAR)	AAR, US DOT
Surface Transportation (Public Transportation)	ST-ISAC	www.surfacetransportationisac.org	01/03	USDOT	American Public Transportation Association (APTA)	APTA, US DOT
Emergency Fire Services	EFS-ISAC	http://www.fema.gov/ppt/reg-v/Plehal.ppt	05/02	FEMA	United States Fire Administration (USFA)	FEMA, USFA
Electricity Sector	ES-ISAC	www.esisac.com	09/00	Department of Energy	North American Electric Reliability Council (NERC)	
Energy (Oil & Natural Gas)	Energy ISAC	www.energyisac.com	11/01	Department of Energy	National Petroleum Council (NPC)	NPC

Table 10 outlines the ISACs that are currently in the planning stages. Some of these industries are identified in PDD-63, while others were formed by additional economic sectors to model the concept of a secure information exchange amongst industry experts.[7]

[7] Some materials in Table 10 are reproduced from Center for Infectious Disease Research & Policy, *Op. Cit.* It should be noted that Table 10 in this chapter has been updated to include information regarding ISACs through July 2003.

TABLE 10: ISACS IN THE PLANNING STAGES

SECTOR	ACRONYM	WEB INFO	START DATE	AGENCY (PDD-63)	SECTOR COORDINATOR	DEVELOPER
Government Services	N/A	www.fedcirc.gov	03/03	Federal Computer Incident Response Center (FedCIRC)	FedCIRC	FedCIRC, Department of Homeland Security (DHS) Information Analysis and Infrastructure Protection (IAIP) Directorate
Aviation	Aviation ISAC	http://www.aci-na.org	03	US DOT	Airports Council International–North America (ACI-NA)	ACI-NA, US DOT
Food	Food ISAC	www.fmi.org/isac	02/02	N/A	Food Marketing Institute (FMI)	FMI
Chemical	Chemical Sector ISAC	http://chemicalisac.chemtrec.com	02	N/A	American Chemistry Council (ACC)	ACC, Chemtrec
Interstate	NASCIO-DHS ISAC	http://www.nascio.org	07/02	N/A	National Association of State Chief Information Officers (NASCIO)	NASCIO

Information Technology ISAC (IT-ISAC)

The information technology sector and the communications industry were both specifically mentioned in PDD-63. The Information Technology ISAC (IT-ISAC) was established on January 16, 2001. It is operated by the Information Technology-ISAC, LLC. This limited liability corporation includes some of the largest and most influential members in the industry including: AT&T; Cisco Systems; Computer Associates; EDS; Hewlett-Packard; IBM; Intel; KPMG; Microsoft; Nortel Networks; Oracle; Symantec; and Veridian.[8] It is designed to facilitate communication among all US-based IT companies and e-commerce firms. The IT-ISAC operation is based at Internet Security Systems in Atlanta, Georgia. Its public website is www.it-isac.org.

Telecommunications ISAC

Telecommunications is identified as a critical sector of the economy in PDD-63. The Telecommunications ISAC is one of the few operated directly by a branch of the federal government called the National Coordinating Center (NCC)[9] for Telecommunications. The

[8] Source of information: http://www.itaa.org/infosec/itisacfaq.htm.
[9] The NCC actually opened for business on January 8, 1984, well in advance of PDD-63.

NCC-ISAC has been operational since January 2000. Decentralized operations exist at each company, linked by an alerting and coordinating network. Information resources related to the Telecommunications ISAC can be found at www.ncs.gov/ncc.

Banking and Finance—Financial Services (FS-ISAC)

Banking and Finance is yet another critical sector identified by PDD-63. The FS-ISAC was the first ISAC to be established, beginning operations in October 1999. It is designed to facilitate communication among banking, finance, and securities organizations. Banks are currently organized to engage in information sharing and have established the defenses necessary to guard against cyber threats. The goal is for every sector within the US economy to be in the same position.[10] The FS-ISAC's public website can be found at www.fsisac.com.

Water Supply ISAC (WaterISAC)

The nation's water supply is identified in PDD-63 as another of the nation's critical industrial sectors. The WaterISAC was made operational in December of 2002. The WaterISAC serves the potable water and wastewater utilities. The WaterISAC is an extension of the Association of Metropolitan Water Agencies (AMWA). It is operated by EWA Information & Infrastructure Technologies, which also operates the Surface Transportation ISAC (ST-ISAC). The WaterISAC is managed through interim operations coordinated by NIPC, FBI, and AMWA and its trade organizations. The WaterISAC's public website can be found at www.waterisac.org.

Trucking ISAC (Truck ISAC)

The American Trucking Association (ATA) created the Trucking ISAC in early 2003, which is responsible for the ISAC's staffing and operations. The Trucking ISAC functions in cooperation with 50 state trucking associations and 15 other national trucking organizations in the Trucking Security and Anti-Terrorism Working Group. This is a more informal arrangement than many ISACs, encouraging truckers that have critical information to contact the ATA. Information resources related to the Trucking ISAC can be found at www.truckline.com/insideata/isac.

Railroad and Public Transportation Sectors—Surface Transportation (ST-ISAC)

The Surface Transportation ISAC (ST-ISAC) was originally developed as an informal communication tool for the Association of American Railroads (AAR). The President of AAR is designated by the Secretary of Transportation as the *Surface Transportation Critical*

[10] Source of information: The White House, Office of the Press Secretary, Remarks by the President in Photo Opportunity with Leaders of High-Tech Industry and Experts on Computer Security, February 15, 2000. This may be found at http://www.politrix.org/foia/unsorted/wh-cybersec.htm.

Infrastructure Sector Coordinator. The United States Department of Transportation (US DOT) initially approached the AAR, after the issuance of PDD-63. Cyber security was the original impetus of PDD-63 and was also of concern to the freight railroads because of their heavy reliance on technology to conduct day-to-day operations. Like many of the ISACs, it was formed out of an original concern for cyber security. Therefore, the ST-ISAC is particularly well equipped to mitigate cyber threats to information systems and technology used by transportation organizations (particularly, the nation's freight railroads).

The AAR, to initiate the protection of physical assets, issued a Request for Proposals (RFP) for professional services, which resulted in a contract being issued to Electronic Warfare Associates Information & Infrastructure Technologies (EWA IIT) of Herndon, Virginia to formally establish and operate the ST-ISAC. The system first became operational in October 2001 in an informal arrangement with Class I Railroads and AMTRAK. Access to this public website can be found at www.surfacetransportationisac.org.

Most recently the public transportation industry has become associated with the ST-ISAC as a sector within surface transportation. APTA is currently serving as the sector coordinator while using all of the existing resources associated with the originally created ISAC. The Federal Transit Administration (FTA) has provided $1.2 million to APTA to facilitate the involvement of all public transportation industry members in the ST-ISAC without direct cost to them. Transit systems are in the process of signing agreements and joining. Public transportation systems operating in the rural and small urban areas that are represented by the Community Transportation Association of American (CTAA) have also been afforded the opportunity to become members of the ST-ISAC under the same umbrella funding.

Emergency Fire Services (EFS ISAC)

The Emergency Fire Services ISAC (EFS ISAC) was established in May 2002. The EFS ISAC represents a partnership between NIPC and the US Fire Administration (USFA), representing the national fire associations, the 50 state Fire Marshals, and over 32,000 local fire and emergency medical departments nationwide. USFA is an arm of FEMA that was given the liaison responsibility for the emergency fire services sector. The EFS ISAC uses the existing dissemination mechanisms of the national fire associations, the 50 state Fire Marshals, and law enforcement networks. More information regarding the EFS ISAC can be found in this PowerPoint presentation: http://www.fema.gov/ppt/reg-v/Plehal.ppt.[11]

Electricity Sector ISAC (ES-ISAC)

The North American Electric Reliability Council (NERC) formed the Electricity Sector ISAC (ES-ISAC) in the fall of 2000. NERC is virtually comprised of all the electric power suppliers

[11] PowerPoint presentation from the FEMA Region V Senior Leaders Homeland Security Summit, Chicago, IL, June 12, 2002.

in the United States, Canada, and a portion of Baja California, and Norte, Mexico. NERC predates PDD-63, as it was formed in response to the Northeast blackout in 1965. NERC's mission is to ensure that the bulk electric system in North America is reliable, adequate, and secure.[12] NERC funds and administers the ES-ISAC. The public portion of the ES-ISAC can be accessed at www.esisac.com.

Oil and Natural Gas Production and Storage—Energy ISAC

The Energy ISAC began operations in November of 2001, covering exploration, production, processing, transmission, distribution, transportation, storage, trading, supervisory control, and e-commerce of energy wares.[13] The sector coordinator for the Energy ISAC is the National Petroleum Council, an advisory committee to the Secretary of Energy on oil and natural gas matters. The American Gas Association, American Petroleum Institute, and National Petro Chemical and Refiners Association are association trustees. The Energy ISAC is funded by a grant from the federal government.[14] The public portion of the Energy ISAC can be accessed at www.energyisac.com.

Continuity of Government Services

The Federal Computer Incident Response Center (FedCIRC) is the agency charged with the Continuity of Government Services, as referenced by PDD-63. On March 1, 2003, the FedCIRC officially became part of the Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) Directorate. FedCIRC is the responsible entity among federal civilian agencies for computer security incident reporting. It also provides assistance with incident prevention and response. The FedCIRC public home page is located at www.fedcirc.gov.

Aviation ISAC

The Airports Council International (ACI) for North America currently hosts a website that provides daily information to professionals in the Aviation industry. It was established in 2003. In response to PDD-63, the ACI-NA is in the process of creating an Airport ISAC consisting of a list-serve system that will allow airports to share information on cyber and physical warnings and threats. Thus far, 33 airports have signed up for inclusion. Additional airports are encouraged to participate in the online forum that is expected to become functional in the coming months. It is being designed to facilitate the secure information exchange among commercial airports, passenger and cargo, in the US and Canada. More information can be found at http://www.aci-na.org.

---

[12] The source of this information is a footnote from: North American Electric Reliability Council, *Before the United States of America, Department of Homeland Security: Procedures for Handling Critical Infrastructure Information, Comments of the North American Electric Reliability Council*, Washington, DC, June 16, 2003.

[13] Source of information: http://www.energyisac.com/faq.cfm.

[14] Ibid.

Food Industry ISAC

On February 15, 2002, the Food Marketing Institute (FMI) and NIPC signed an agreement creating a partnership with the Food Industry ISAC, with FMI serving as the central party. FMI represents supermarket owners. The Food Industry ISAC is intended to:

- ❒ provide data and analysis allowing the food industry to report, identify, and mitigate its vulnerability to attack, and to recover from any attacks as quickly as possible;
- ❒ help NIPC and FBI identify threats meriting attention and create specific warning messages appropriate to the food industry; and
- ❒ lend expert, industry-versed assistance to the FBI in evaluating specific threats.[15]

The public portion of the Food ISAC can be accessed at www.fmi.org/isac.

Chemical Sector ISAC

Chemtrec, the chemical industry's 24-hour emergency communication center, and the American Chemistry Council, in cooperation with NIPC, established the Chemical Sector ISAC. The Chemical Sector ISAC, created in 2002, is intended to support companies or organizations manufacturing, storing, transporting, distributing, or handling chemical products. The ISAC uses email and a secure website to communicate with members and allows members to voluntarily and securely report malicious, unexplained, or suspicious incidents involving chemical facilities or chemicals in commerce.[16] The public site for this ISAC can be accessed at http://chemicalisac.chemtrec.com.

NASCIO-DHS Interstate ISAC

In July 2001, the National Association of State Chief Information Officers (NASCIO) formed the *NASCIO-DHS Interstate ISAC Information Sharing Program*. This appears to be an email distribution network for transmission of perceived common threats. Members may alert NIPC of incidents directly. Sanitized NIPC reports, appropriate to state information technology interests, are forwarded to contacts in each of the 50 states, which may then elect to distribute the information more widely. More information regarding NASCIO and its role in securing the communication infrastructure can be found at http://interstate-isac.nascio.org.

ISAC PURPOSE

Critical industries have initiated ISACs for a variety of reasons. The most important of these are:

---

[15] Source of information: http://www.fmi.org/isac/.
[16] Source of information: http://chemicalisac.chemtrec.com/ChemIsac.nsf/chemical_sector.

- ❒ the opportunity to share information among similar enterprises;
- ❒ the potential to receive early warnings of threats;
- ❒ industry coordination and pattern recognition;
- ❒ public and private cooperation in a non-FOIA environment; and
- ❒ avoiding security-related government regulation.

Information Sharing

Perhaps the most important purpose of an ISAC is the prospect of information sharing within an industry. The types of information shared in an ISAC environment are likely to be:

- ❒ best security practices (lessons learned);
- ❒ shared experiences;
- ❒ background information on threats;
- ❒ resources; and
- ❒ contacts.

Best Security Practices

Best security practices can come from a variety of sources and relate to items such as planning for emergency incidents, mitigation, response, and recovery. These may be drawn from industry literature or studies. Reference to these items may be communicated by on-line secure bulletin boards or mentioned as lessons learned in discussion forums, chat rooms, and through direct responses to member inquiries. For obvious reasons, it is desirable to share such material in a secure environment, especially when such practices are attributable to a specific member or class of members.

Shared Experiences

This is an area where discussion forums or chat rooms in a secure environment can be extremely productive. Discussion forums may be segregated into specific subjects as well, so individuals concerned mostly about, for instance, bridge security, can solicit ideas without having to read through information or questions pertaining mostly to tunnels. It seems that this is an area where a public sector ISAC could excel. For example, New Hampshire Turnpikes are not in competition with the New Jersey Turnpike (NJT) and would benefit from information received from NJT. If there are better ideas to be obtained, sharing them only increases the robustness of the national network. Clearly, not everyone will discover the same set of problems as the effects of winter cold in Northern Minnesota or the damages caused by summer heat in Southern New Mexico to pavement-imbedded security devices. At the same time, creating a broad electronic community of security-minded operators appears to have merit. Creating a secure forum to discuss operational security matters appears to be prudent and, for the public sector, auspicious in its potential effectiveness.

Background Information on Threats

Often a feature of an ISAC is an abundance of background information regarding threats. This information is not so true for threat warnings or alerts, but rather background information on events or information that may raise awareness to threats. In an ISAC environment, much of this information is likely to be open-source and available from other venues, if one chooses to initiate a search. The advantage the ISAC brings is consolidating this information in one place, usually on a secure website, but sometimes included in the ISAC's email messages. In the case of the ST-ISAC, sorting information of this nature from other, more critical, messages has been a part of the ISAC's evolution. Users, particularly in the public transportation sector, have expressed a preference to have critical information segregated from the general information in a way that it can be quickly referenced.

Resources

Resources can span a considerable gamut of available information. Among the items considered as resources for an ISAC are:

- ❒ databases populated with significant historical threat data to assist members in interpreting current circumstances;
- ❒ recent topical studies or other on-line resources;
- ❒ current articles on subjects of interest to ISAC members;
- ❒ significant executive or legislative actions, documents, or requirements that may impact the membership of the ISAC or parts of its operation; and
- ❒ sensitive notifications, analyses, or other information that can be posted on a secure website, but are too sensitive to be disseminated by even secure email.

Many of these items may be posted on the secure website by the ISAC operator, for the benefit of its members. Additionally, these members can usually post items themselves by way of a membership bulletin board or in reference to items in a discussion forum.

Contacts

In the current security environment, and especially in the wake of significant emergency events, key individuals, their contact information, and the specific circumstances in which they can be contacted is often judged as information that is too sensitive to be openly available to the general public. These individuals could become potential targets. This is where the ISACs role as a central source of information can be particularly valuable. Contact information for counterparts in other organizations can be useful, but is not always easy to obtain. Therefore, this information should be gathered as a proactive task, prior to any security-related incident, and be made available to decision-makers when appropriate and necessary. In addition, ISACs can be useful repositories for identifying which agencies have responsibility for different parts of the security apparatus and providing additional valuable web links, names, titles, phone numbers, email addresses, and other contact information.

Early Threat Warning

Another viable purpose for creating and operating an ISAC or becoming a sector coordinator member of an existing ISAC is to receive early warnings of threats. This is certainly true in the case of cyber threats, as the principal operators of ISACs are well connected to the cyber security world and are constantly vigilant about the prospect of attacks to the information technology sector.

Even the most ardent supporters of the ISAC purpose would not contend that involvement in an ISAC would prevent an organization from falling victim to a cyber attack. The best that can be expected is that another organization might be the first target of an attack and others would become alerted to the new threat as soon as possible thereafter. Many operators of ISACs are well versed in these situations and are capable of monitoring the attempts of outside parties to gain access to a particular system or network. They are also quite skilled at developing quick security patches and defenses and in rapidly disseminating information regarding specific threats.

The situation regarding the prospect for physical attacks, though more complex, may not be as optimistic as that of cyber threats. While there are certainly successes in anti- and counter-terrorism, seldom do those interested in perpetrating evil absent-mindedly leave maps and plans of their intentions lying out in the open. More often, the hope for those involved in protecting physical infrastructure is to get as much and as specific information as possible about potential targets (conduct a critical asset inventory), share information regarding the most effective manner to harden those assets and make them less attractive, and the best steps to implement in responding to an identified threat. An ISAC can help in this regard by sharing methodologies, best practices, and threats received by the industry and providing additional tools to aid with an organization's preparation and coordination with other entities performing the same functions. An ISAC involvement and due diligence regarding ISAC, FBI, Joint Terrorism Task Force, and other association reports may raise enough awareness for the industry to effectively prevent attacks by responding to security-related threats, and mitigating the effects of those which cannot be prevented.

Industry Coordination and Pattern Recognition

The banding together of organizations with similar business or governmental purposes may be one of the most important and promising aspects of forming an ISAC. One organization alone cannot create an impregnable fortress and still conduct normal business practices. However, organizations within the same industry can conduct business freely, and still protect their business methodologies, practices, and interests, while administering, partnering with others, or having membership with an ISAC. Free interchange of information with both known and unknown individuals is part of the necessary routine for any public or private entity. To cease those interactions is to surrender to possible threats. Therefore, the question is not how to become 100 percent secure because that is impossible, but rather, how to maximize security at the right times and in the right places in order to prevent

attacks, if possible, and if attacks occur, to appropriately respond and recover. Operating or participating within an ISAC facilitates both the prevention and mitigation processes.

As available and exchanged information may not be entirely accurate, it seems logical that organizations engaged in similar efforts to protect their critical infrastructure may prefer to be in contact with one another to strategize and compare threats, responses and experiences. An ISAC is, perhaps, one of the best available secure and organized opportunities for achieving this objective. Discussion might, to ensure accuracy, take place through ordinary telephone correspondence or teleconferencing. It may also be electronically facilitated through the use of secure chat rooms or discussion forums, and/or a virtual private network (VPN).

The ST-ISAC has made heavy use of a simple device called Zixmail that, for a nominal annual fee for each member, creates secure email transmissions from messages that might otherwise need to be transmitted by other means.[17] This type of service is available from vendors who have no connection to the ST-ISAC. However, forming a community of critical-industry members under the ISAC umbrella encourages this kind of mutual dialogue by whatever technological or physical means necessary to achieve two-way communication. A similar system with the trade name Bantu has been acquired by the Department of Homeland Security and distributed to 5,000 first responder units. Emails sent over the Bantu system are also encrypted and distributed over a system that contains firewalls.[18]

One of the continuing arguments in support of ISACs has been the concept that more is better. This is certainly true in the context of ISAC finances, which is discussed later in this chapter. Having more information available to analyze can help with determining trends, establishing patterns, and assessing the thrust of received threats. Attacks to the critical infrastructure may begin in one sector, but may really be a part of a much larger plan with far more devastating objectives, as was demonstrated on September 11. From this perspective, a broader viewpoint is better. It allows for analysts to establish that a pattern exists or that the actions of a plan are emerging. Once established and verified, this information can and generally is made available to all ISAC members.

However, this argument may not be as true in the case of cyber threats. Here, the distinctions of critical industry sectors may not be particularly meaningful.[19] There are differences in information technology structures and security protocols from one

[17] Zixmail is a product of Zixcorp. The National Cooperative Highway Research Board, Transportation Research Board and McCormick Taylor Research Team do not endorse any product or manufacturer.

[18] The National Cooperative Highway Research Board, Transportation Research Board and McCormick Taylor Research Team do not endorse any product or manufacturer.

[19] This viewpoint was articulated by Christopher Dixon, Digital Government Issues Coordinator, at the National Association of State Chief Information Officers (NASCIO) in a telephone interview conducted on July 3, 2003 by McCormick Taylor's Peter N. Bromley.

organization to another and likewise among critical industry sectors. However, one of the fundamental foundations of the ISAC movement, particularly with respect to cyber threats, is the degree of shared vulnerability, regardless of organization and even the industry. For example, the same private company, as a contractor to the ISAC organization, operates and manages both the ST-ISAC and WaterISAC. Cyber attacks in any of these industries, if successful, will certainly have different effects within an industry or an organization, but the attacks themselves may come from the same worms, viruses, or other malicious transmissions. This is why these same ISAC operators have an established level of competency in an area that essentially overlaps critical industries. Many of the threats they uncover in the cyber world are capable of affecting anyone with a computer connected to the Internet or to another computer via the electronic or physical exchange of information. At the same time, it is also possible for more organized evildoers to target a selected sector or particular enterprise for a cyber attack with unknown, but potentially scary, repercussions. An orchestrated attack on any number of enterprises is liable to be more quickly detected if all sites of impact are closely monitored.

In contrast, one could argue that the same system operator for a number of ISACs would themselves become a target for attack since crippling their functional capabilities could take down the defensive and responsive abilities of multiple sectors within the critical infrastructure economy. One could also argue that infiltration into the personnel ranks of a multiple ISAC provider of only one perpetrator could potentially serve to take down all of the affiliated ISACs.

Anonymous Information Sharing

Anonymous information sharing, for some businesses, may be the principle purpose for becoming a member of an ISAC. In the private sector, admission that a particular organization has been the victim of a cyber or physical attack may be more than just embarrassing. In many cases, for such information to become public might have the effect of driving business away or reducing the market value of the corporation's stock. For instance, the Tylenol crisis in 1982 was highly publicized. The immediate effects to the Tylenol product line were devastating as a result of the negative publicity, not from any product failures. Mitigation of the problem was achieved through a textbook example of effective communication and public relations: the company initiated appropriate action and recalled all of the products that were being sold at that time. Johnson & Johnson was very lucky in that the company did not lose future sales for Tylenol as well. If Johnson & Johnson did not implement effective public relations to follow up with this event, customers could have easily viewed the company as vulnerable to attacks in the future. For this reason, the ability to cite security-related concerns, particularly negative ones, in an anonymous manner is appealing to many organizations. However, many argue that the ability for ISAC members to be able to provide input anonymously opens the door to inaccurate or non-verifiable information that indeed may be incorrect. The dissemination of bogus information, even if it was thought to be correct by the submitter, can have a significant negative impact to the members receiving the information and who take counteraction steps that are costly and ineffective.

Another supporting reason for the value of anonymity, particularly in regulated industries, is that many government agencies with lead responsibility for industrial sectors under PDD-63 (e.g., the EPA is the liaison agency for the water and wastewater industries) are the same agencies charged with ensuring that companies within the industry are obeying and following the law. Many companies worry that sharing any information, in an attributed form, with the agency responsible for regulating them creates a conflict of interest.

Most analysts admit that receiving too much information is more preferable than receiving too little or no information regarding an expected or occurring attack. For this reason, an unattributable report outweighs the complete absence of information. However, the debate on this issue should be furthered. The ultimate question is whether or not AASHTO is willing to lead or be part of an ISAC that accepts and disseminates anonymous information.

Public and Private Cooperation in a Non-FOIA Environment

The issue of non-application of the Freedom of Information Act (FOIA) to ISACs is similar to the previously cited issue of attributed reports. One of the underlying purposes of PDD-63 is to acknowledge the degree to which government and private industry, in critical sectors, have a symbiotic relationship regarding the issue of security. Government officials understand that they lack the expertise in managing these critical industries to effectively secure the nation's critical infrastructure. Concurrently, there is a perceived need for the industry to direct greater awareness and attention to security issues, for the protection of individual organizations as well as whole industry sectors and the national economy.

Regarding proprietary interests, private industry's reluctance to share this information is understandable. The information exchange within ISACs (by the known interpretations to date) is not subject to disclosure under the Freedom of Information Act. From the standpoint of many entities, this allows for the considerable advantage of the government's assistance to conduct security measures, without risking the revelation of proprietary information. The government prefers owners and operators who have little to fear regarding proprietary information to be more forthcoming in sharing important facts regarding security problems and concerns.

Avoiding Security-Related Government Regulation

One guideline of PDD-63 states that critical infrastructure protection should be market-driven and voluntary, rather than regulatory. However, the directive also included the key clause that regulation should only be used *in the face of a material failure of the market to protect the health, safety and well being of the American people*.[20] For many sectors, this is a clear message. Information gleaned through various sources indicates that owners and operators of critical industries have been very concerned about the prospect of government regulation mandating them to engage in onerous or counter-productive security practices. By joining

[20] The White House, *Presidential Decision Directive 63*, Op. Cit.

an appropriate ISAC, organizations are voluntarily participating in critical infrastructure protection as actively or inactively as they choose.

ISAC ROLE

The role of an ISACs should be understood at three levels:

- ❒ cyber versus physical threats;
- ❒ within an industry sector's overall security construct; and
- ❒ within an individual organization's or an ISAC participant's system security plan.

Cyber Versus Physical Threats

The role of an ISAC in communicating and responding to cyber threats is well known, valued, and understood. Some ISAC operators (competitively selected private contractors) are among the most proficient in identifying and monitoring cyber threats.

However, their experience in understanding the physical and operational aspects of the businesses they are now helping to protect has, on many occasions, been seriously questioned. In response, attempts have been made to educate contractor analysts working for the ISACs about the industries with which they are associated.[21] This is a concern to many potential ISAC participants, since they are literally purchasing the services of a contractor who may know very little if anything about the conduct and operation of their critical enterprise. The analogy is that a medical doctor trained and practiced in the ear, nose and throat proficiency area would immediately recognize related symptoms and trends within this specialty but would have limited capability in successfully diagnosing and, perhaps, understanding an orthopedic problem.

In the case of the ST-ISAC, industry experts have formed a working group with analysts to help give meaning, from a knowledgeable industry perspective, to threats that the ISAC operator receives. Within the working group, industry experts train analysts to see how specific information may be pertinent to that sector's physical security. It is debatable as to whether converting a primary defense contractor, practiced in cyber security, to the physical and operational ways and means of the highway transportation industry is more appropriate than hiring security practitioners who are already proficient in the security aspects of highway transportation.

Software systems and expertise to ward against cyber threats can be sold to any industry concerned with technological security. Technical knowledge regarding an industry's physical vulnerabilities may not be as abundantly available. Analysts and operators with

[21] For example, Greg Hull of the American Public Transportation Association (APTA) created a course for the ST-ISAC's analytical contractor employees. Similar introductions to the industry have been conducted for the WaterISAC's analytical contractor employees.

industry training or experience should be considered valuable assets to the ISAC that AASHTO may want to create or join.

Within an Industry Sector's Security Construct

In creating PDD-63, the government realized that every industry has a different approach to communicating security-related concerns. It would not be possible to group these sectors together under one secure communication plan or ISAC.

The first ISAC to become truly operational was the Financial Services ISAC. This was intentional, as the original role of the newly created ISAC concept was to monitor attempts to impinge electronic financial accounts. While PDD-63 briefly discussed the issue of physical security, it was primarily oriented toward the issues of cyber security, due to the publicity regarding a variety of destructive viruses and hacker attempts at the time it was issued.

The Financial Services industry prospers today through the strength of its technological and information systems. Physical instruments representing currency and other documents that can be exchanged for money, such as stock certificates, occupy a smaller share of the transactions that take place today. Nowadays, individuals are paid instantaneously via electronic wire transfers, again, making the information systems of the financial industry more vulnerable.

In contrast, this is probably less true of many small public transportation systems, for example, that may only be connected to the Internet by means of the General Manager's private account. These systems, if they are security-minded, are mostly concerned about threats to their physical security. Some physical security breaches that may destroy the system's credibility with the riding public include:

- ❒ bus hijackings;
- ❒ hostage taking;
- ❒ vandalism; and
- ❒ other random or conspired acts of violence against their physical plants, vehicles, passengers and employees.

These systems may be on the other end of the technology spectrum from the financial industry, preferring to receive security information that helps them protect their physical assets and passengers as opposed to their electronic transactions. If an ISAC could provide advanced warning regarding a vulnerable location or asset, these public transportation systems would definitely benefit from membership. In this case, threat warnings concerning cyber security are not as valued as those regarding aspects of physical security.

The industries previously mentioned are spread across the spectrum of cyber versus physical security. However, there are sectors with critical and sophisticated information technology systems, whose compromise could indirectly be life or property threatening,

that also are concerned about their significant physical assets, such as dams or nuclear plants.

Within an Individual Organization's or an ISAC Participant's System Security Program

It is very clear, regarding security measures, that one size does not fit all. Security plans need to have many of the same common elements, but clearly, the method by which vulnerabilities are identified and resolved will vary specifically within each organization or industry, though some of the same general techniques may be employed.

Likewise, the role of an ISAC can vary in importance from one organization to another, even within the same industry. A larger organization, perhaps in an urban environment, may have many resources to obtain threat information, such as independent informants reporting to metropolitan police, local FBI offices, local secret service offices, a Joint Terrorism Task Force, and perhaps even sources from within its own security forces. A smaller organization, perhaps in a rural environment, may need to be very self-reliant for its information. The role of an ISAC may prove to be critical in the latter case in which a smaller organization has fewer credible resources. However, large organizations can also benefit from incorporating its ISAC membership into the overall system security program by comparing ISAC reports to information gleaned from other reliable sources.

REFERENCES

FEATURES CATALOGUE

Balog, John N.; Bromley, Peter N.; Strongin, Jamie Beth; Dattilio, Daniel J.; Boyd, Annabelle; and Caton, James, *Preliminary Draft Final Report: Evaluation of the July 3, 2002 Integrated Transportation Analysis (ITA) System Demonstration, NCHRP Project 20-59(10)*, McCormick, Taylor & Associates, Inc., National Cooperative Highway Research Program, Transportation Research Board, Washington, DC, July 22, 2002, unpublished.

Balog, John N.; Boyd, Annabelle; Bromley, Peter N.; Caton, James; Dattilio, Daniel J.; and Strongin, Jamie Beth; *Secure Communication Infrastructure Phases 2 and 3, Task 4A, Preliminary Draft Final Report on Tasks 1 and 2*, NCHRP Project 20-59(10), McCormick, Taylor & Associates, Inc., National Cooperative Highway Research Program, Transportation Research Board, Washington, DC, March 10, 2003, unpublished.

Department of Commerce, National Institute of Standards and Technology, Office of Law Enforcement Standards; Department of Justice, National Institute of Justice, AGILE Program; and Department of Homeland Security, Science and Technology Directorate, SAFECOM, *Briefing Book of Public Safety Related Groups and Programs on Interoperable Communications and Information Sharing*, Summit on Interoperable Communications for Public Safety, Office of Management and Budget, Washington, DC, June 26–27, 2003.

Crystal Reports website:
http://www.crystaldecisions.com/products/crystalreports/default.asp

SunGard Business Continuity and Internet Services home page:
http://www.sungard.com.

Disaster Management Interoperability Services home page:
http://www.cmi-services.org.

E-Gov Initiatives at a Glance at
http://www.whitehouse.gov/omb/egov/downloads/E-Gov_Initiatives.pdf.
http://www.cmi-services.org/services.asp

Techno-Security Conference website:
http://www.techsec.com/html/Techno2003.html.

New Mexico State Highway & Transportation Department Research Bureau, *Integrated Transportation Analysis Procedure Manual*, Albuquerque, NM, December 2002, unpublished. This is a “Sensitive, Need-to-Know Information” document. It contains “Restricted, Need-To-Know Information.” Its contents cannot be reproduced or distributed without prior permission from David Albright, Director, NMSHTD Research Bureau, 1001 Blvd., SE, Suite 103, Albuquerque, NM 87106.

Global Justice Information Network Annual Report 2002, http://www.it.ojp.gov/global/outreach/37/global_report_2002.doc.

Institute for Intergovernmental Research, Regional Information Sharing Systems Program, *The RISS Program: 2001, Membership and Service Activity,* Tallahassee, Florida, July 2002, http://www.iir.com/Publications/RissProgram2001.pdf.

IMPLEMENTATION OPTIONS ASSOCIATED WITH THE ESTABLISHMENT OF AN AASHTO HIGHWAY TRANSPORTATION ISAC

The White House, *Presidential Decision Directive 63*, Washington, DC, May 22, 1998.

The White House, President George W. Bush, *Executive Order 13231: Critical Infrastructure Protection in the Information Age*, Washington, DC, October 16, 2001.

Center for Infectious Disease Research & Policy, *Critical Infrastructure ISACs*, University of Minnesota, August 2002, http://www.cidrap.umn.edu/cidrap/files/20/table-isacs.pdf.

ITAA's InfoSec home page: http://www.itaa.org/infosec/itisacfaq.htm.

The White House, Office of the Press Secretary, Remarks by the President in Photo Opportunity with Leaders of High-Tech Industry and Experts on Computer Security, February 15, 2000. Found at http://www.politrix.org/foia/unsorted/wh-cybersec.htm.

PowerPoint presentation from the FEMA Region V Senior Leaders Homeland Security Summit, Chicago, IL, June 12, 2002.

North American Electric Reliability Council*, Before the United States of America, Department of Homeland Security: Procedures for Handling Critical Infrastructure Information, Comments of the North American Electric Reliability Council*, Washington, DC, June 16, 2003.

Energy ISAC home page: http://www.energyisac.com/faq.cfm.

Food and Agriculture ISAC home page: http://www.fmi.org/isac/.

Chemical Sector ISAC, http://chemicalisac.chemtrec.com/ChemIsac.nsf/chemical_sector.

Financial Services ISAC home page: http://www.fsisac.com/faq.cfm.

Presentation by Stash Jarocki, FS-ISAC Chairman, NASCIO Meeting, March 8, 2002. From https://www.nascio.org/2002/03/StateISAC020308.cfm.

WaterISAC, *Subscription Agreement for Individual Systems*, Washington, D.C., May 2003. Found at http://www.waterisac.org/IndividualSystemsAgreement.pdf.

APPENDIX A: THE INTEGRATED TRANSPORTATION ANALYSIS (ITA) SYSTEM

SUMMARY

The Integrated Transportation Analysis (ITA) system has been a cooperative venture primarily involving the New Mexico State Highway and Transportation Department (NMSHTD) and Sandia National Laboratories (Sandia). It has been designed to serve as a **communication device** that will allow real-time posting and communication of actual information on natural and intentional emergencies for distribution among states and other agencies including the federal government and law enforcement agencies. Currently no other system exists, despite the definite need, particularly in this post September 11 environment.

The ITA system is further conceived to provide an extensive array of analytical capabilities in support of the basic communication component so that collected information can be used to forecast a developing terrorism event. This would allow managers and decision makers the opportunity to interdict or mitigate the negative intensity and aspects of the oncoming event.

The communication aspects of the ITA system are more fully developed than the analytical aspects. The demonstration of the ITA system on July 3, 2002 was primarily designed to evaluate whether four communication competencies could be established. Competencies associated with the analytical capabilities were not tested. To the extent that they were conceptually included, observers in 13 locations were exposed to what could be expected in a future version of the ITA system.

The four communication competencies were established during the demonstration. The ability for individuals to call into the Call Center to convey the presence of a threat, and to distribute this and follow-up messages in a secure manner via a Virtual Private Network (VPN) to the five participating states and the seven other agencies including the FBI and the US Department of Transportation (USDOT) was successful.[1] In addition, the ability to use a secure website as a repository for all communications and to use the geographic information systems (GIS) to display information necessary to develop and effect a response to an incident was established.

[1] Participants in the ITA system demonstration were the United States Department of Transportation (US DOT), Transportation Information and Operations Center (TIOC), in the District of Columbia; Maryland State Highway Administration (MDSHA), near Baltimore, Maryland; Texas Department of Transportation (TXDOT), in Austin, Texas; Washington State Department of Transportation (WSDOT), in Olympia, Washington; Federal Bureau of Investigation (FBI), National Infrastructure Protection Center (FBI-NIPC) in Washington, DC; United States Department of Transportation, Federal Highway Administration (FHWA) District Office in Texas; New Mexico State Highway and Transportation Department (NMSHTD) General Office; the FHWA District Office in New Mexico, NMSHTD District Six in Grants/Milan, New Mexico; the Albuquerque Call Center site at the New Mexico State Police (NMSP); the New Mexico State Emergency Management Center; the Albuquerque Field office of the FBI, and the Sandia National Laboratory.

In the judgment of the McCormick Taylor Quick Reaction Research Team (McCormick Taylor Research Team**)**, the current version of the ITA system demonstrated the minimum core competencies desired and claimed before the demonstration, at least in a limited application. Some ITA demonstration sites performed flawlessly.

The ability of the ITA system to act reliably in a sustained manner has not yet been proven. It should be noted that reliability and sustainability issues are technical concerns that can be expected to be resolved in the future and were not targeted as competency areas. Unfortunately, the reliability and sustainability attributes were troublesome enough to distract from the fact that the four targeted competencies were established.

Success always helps in identifying the additional advancements that are needed. The ITA system's apparent current deficiencies and expansion capabilities are discussed in some detail in the remaining subsections of this appendix. Rather significant recommendations regarding the following interest areas are identified and discussed:

- ITA public domain system;
- ITA virtual private network connectivity;
- ITA connectivity with other management information systems;
- ITA system details;
- ITA call center and notification;
- ITA messaging and website communication protocols;
- ITA user-friendliness;
- ITA user resource databases;
- ITA outreach and training;
- ITA costs; and
- other ITA findings.

It should be noted that the ITA system currently offers considerable value to all potential users. It also possesses a significant amount of positive and valuable concepts associated with the analytical component that need to be further explored as research and development topics. The analytical component is the least developed and the most difficult to mature through the research process. In other words, significant challenges remain with respect to making the identified concepts functional during real life applications. These challenges are expected to be addressed and overcome; however, it will take a considerable amount of time, perhaps years, to do so.

In contrast, the communication component is currently more fully developed and as a result offers the potential for expanded functionality in the nearer future. Considering that immediate transportation industry needs are in the communication area and the ITA system is currently somewhat functional, it is recommended that immediate future research and development work be primarily conducted on the communication component. This work should be greatly associated with the development of the functional requirements for the ITA system. This means that all necessary steps that can be sustained with the remaining budget of this task order should go toward forwarding the concept and specifying the functionality of the ITA system. These functional requirements can then be turned over to

the programmers, so that they can develop the code that allows for the achievement of the specific attributes of the system. Any remaining task order resources could then be directed to the development of the functional requirements for the analytical component of the ITA system.

Three primary steps are recommended for the initial application of the available task order resources. The first involves presenting the findings of this effort on the task order to the National Cooperative Highway Research Program (NCHRP) Panel. This will allow the McCormick Taylor Research Team and the Panel to discuss the opportunities for continued research so that prioritization of topics can be established for the remaining funding and time budgets. The second involves interactions with members of the National Panel that was alluded to in the Request for Proposal for this Task Order so that their priorities can also be established.[2] The third involves identifying all similar systems and collecting enough information on them, so that their positive functions can be documented. This list can then be evaluated for potential inclusion and prioritization in the functional requirements of the expanded and enhanced ITA system. The McCormick Taylor Research Team believes that extensive involvement with the NCHRP Panel will be necessary.

The current version of the ITA system offers considerable conceptual capability regarding the needs of the transportation industry. It also offers some communication functionality that can be implemented in the near future. Over the longer run, it can be enhanced to include significant analytical capabilities that will substantially improve its ability to predict or forecast events so that prevention or mitigation can be realized.

Proof of concept has been achieved. Taking the next steps will contribute to providing the transportation industry with an effective tool for addressing the natural and intentional emergencies that will be present in the future.

INTRODUCTION/ORIENTATION

The initial task order on this program was to participate in a demonstration of the Integrated Transportation Analysis (ITA) system and to provide an impartial, objective evaluation of its ability to satisfy four communication competencies. This system was originally developed in a cooperative effort among the New Mexico State Highway and Transportation Department (NMSHTD), Sandia National Laboratories (Sandia), the Department of Energy, and Veridian to provide a communication system linking state and federal transportation entities for the purpose of sharing real-time emergency and intelligence information related to environmental challenges, such as hurricanes, floods, and forest fires, and security events, such as terroristic actions. The ITA system also has the capability of including emergency responders and others in the secure communication network. The communication aspects of ITA were developed sufficiently to conduct a

[2] The NCHRP Panel will be responsible for deciding on the merit of a National Panel.

multi-state and multi-entity proof of concept test, the primary goal of this initial task on the program and the topic of discussion for this appendix.

The ITA system has also been conceived to include an analytical component that is expected to ultimately possess the capability of forecasting potential terrorism events, so that they can be prevented, mitigated, or otherwise addressed in the most effective manner.

This introduction/orientation subsection summarizes the activities involved in the evaluation.

ITA SYSTEM SOFTWARE TRAINING

Six members of the McCormick Taylor Research Team invested nearly three days on-site at the ITA Command Center in Albuquerque, New Mexico, in the latter part of June 2002, to maximize their familiarity with the ITA system and to receive training on all possible facets of its software.

DEVELOPMENT OF STRUCTURED TOPIC GUIDES

Structured topic guides for conducting interviews with key stakeholders were designed after the New Mexico training to gather perceptual information regarding the expectations of the ITA system prior to the demonstration, and the successes and failures of the program immediately following the July 3 demonstration. These topic guides served as rubrics for gaining crucial knowledge of the functionality of the ITA system by documenting the understanding and experiences of the stakeholders who are responsible for working with ITA on a daily basis or who have a professional interest in the potential usefulness of the ITA system in their agency.

A copy of the content of the pre-demonstration structured topic guide is included as Exhibit A-1 near the end of this appendix. The content of the post-demonstration structured topic guide is included as Exhibit A-2 at the end of this appendix.

PRE-DEMONSTRATION INTERVIEWS

Six McCormick Taylor Research Team members each invested three days at respective locations of ITA system workstations in the states of Maryland, Missouri, New Mexico, Texas and Washington, and in Washington DC at the US Department of Transportation's Transportation Information Operations Center (TIOC). The first two days were primarily associated with conducting expectation and functionality interviews with the local stakeholder participants. One of the purposes of these preliminary interviews was to establish the perceived pros and cons of the ITA system prior to the July 3 demonstration. These could then be contrasted with the actual performance of the system during the demonstration.

The interviews were conducted on-site and face-to-face with key individuals within the state DOTs, federal agencies, and those most closely associated with developing and

using the ITA system. Information gathered from these interviews and discussions was used in the development of the findings reported later in this appendix.

Table A-1 lists all of the professionals interviewed by the McCormick Taylor Research Team as part of the demonstration evaluation process.

EVALUATIVE OBSERVATIONS

One member of the McCormick Taylor Research Team was present during the demonstration of the ITA system at each of the six spatial locations. Each member had previously established a working knowledge of the ITA system and a reasonable understanding of the expectations of each of the representative stakeholders. Each team member observed the demonstration, monitored the discussion of participating stakeholders, and recorded their observations.

By observing, taking notes, and recording the event or series of events in a journal at each of the on-site location states, impressions as to the functionality, ease of use and problems associated with the ITA system during the demonstration were recorded. This information was used in the development of the findings reported later in this appendix. This information also proved valuable during the post demonstration interviews, conducted by telephone, with the professionals who participated in the original demonstration.

POST DEMONSTRATION INTERVIEWS

The available budget dictated the need for the post demonstration interviews to be conducted via telephone. All post demonstration interviews were completed during the week following the July 3 demonstration to ensure accuracy and timeliness. All professionals interviewed prior to the ITA system demonstration were contacted. Interviews were completed with all of those who were available during this period. The post demonstration structured topic guide[3] was used during the interviews.

THE APPENDIX

This appendix:

- ❒ summarizes the findings from the evaluation of the ITA system demonstration and addresses the experiences of transportation professionals from all over the country who participated in the July 3 demonstration; and

- ❒ includes a Draft Work Plan for the conduct of additional activities associated with the ITA System in order to advance its communication and analytical capabilities in satisfying the needs of all transportation systems.

[3] A copy of the content of the post demonstration structured topic guide developed and utilized by the McCormick Taylor Research Team is included as Exhibit A-2, later in this appendix.

TABLE A-1: PROFESSIONALS INTERVIEWED AS PART OF THE JULY 3, 2002 DEMONSTRATION OF THE ITA SYSTEM

NAME	TITLE	ORGANIZATION
Jerry Amato	Division Administrator, Federal Motor Carrier Safety Administration	US Department of Transportation, Washington Division
Sherrie D. Anderson	Program Manager, TSA Maritime/Land Security and Passenger Security	US Department of Transportation, Office of the Secretary
Tehran Anderson	Transportation Specialist	Federal Highway Administration, Office of Transportation Operations
Larry L. Austin	Chief	New Mexico Department of Public Safety, Office of Emergency Services and Security
Rico Baroga	Map-Decision Support Manager	Washington State Department of Transportation
Alfonso Benet	Highway Engineer	Federal Highway Administration, Office of Transportation Operations
Janet K. Benini	Deputy Director	US Department of Transportation
Timothy E. Bradbury	Support Branch Manager	Texas Department of Transportation, Bridge Division
William Brown	Intelligent Transportation Systems (ITS) Engineer, OSC Headquarters	Washington State Department of Transportation, Traffics Division, Advanced Technology Branch
Brian P. Carney	Operations Chief	US Department of Transportation, Office of Emergency Transportation
Lyle Cates	Consultant	Cates Computer Services
Rick Chavez	Highway Operations Engineer	New Mexico State Highway and Transportation Department
John Contestabile	Director, Office of Engineering and Procurement	Maryland DOT

TABLE A-1: PROFESSIONALS INTERVIEWED AS PART OF THE JULY 3, 2002 DEMONSTRATION OF THE ITA SYSTEM

NAME	TITLE	ORGANIZATION
Jim Daily	Maintenance Support Branch Manager	Texas Department of Transportation, Maintenance Division
Mike Ellis	Map Support Specialist	Washington State Department of Transportation
Arthur J. Gottlieb	Inspector General	State of New Mexico Highway and Transportation Department
Joe Graff	Maintenance Section Director	Texas Department of Transportation, Maintenance Division
John Harris	Transportation Security Specialist	US Department of Transportation, Office of Emergency Resources
Steve L. Harris	Emergency Operations Center Operations	New Mexico Department of Public Safety, Office of Emergency Services and Security
Steven P. Harris	District Engineer, District III	New Mexico State Highway and Transportation Department
Tom Hicks	Director, Office of Traffic and Safety	Maryland State Highway Administration
Gale L. Hines	Program Assistant	US Department of Transportation, Research and Special Programs Administration
Jackie Hood	Professor and Director	Transportation Management Research Center (T-MARC)
Rick Horton	Information Technology Systems Specialist	Washington State Department of Transportation
Scott Jones	Information Systems Manager	New Mexico Department of Public Safety, Office of Emergency Services and Security
Paul Jordan	Analyst Supervisor	Texas Department of Public Safety Counter-terrorism Unit

TABLE A-1: PROFESSIONALS INTERVIEWED AS PART OF THE JULY 3, 2002 DEMONSTRATION OF THE ITA SYSTEM

NAME	TITLE	ORGANIZATION
Michael Kline	Information Systems Security Branch Manager	Texas Department of Transportation, Information Systems Division
Bill Klipple	Infrastructure Support Branch Manager	Texas Department of Transportation, Information Systems Division
Ed Leacock	Colonel, Senior Intelligence Officer	Army National Guard
Timothy W. Manning	Director, Emergency Operations Center	New Mexico Department of Public Safety, Office of Emergency Services and Security
Alvin Marquess	Manager, CHART Operations	Maryland State Highway Administration
Stan Mattingly	Research and Technology Engineer	FHWA in Albuquerque
Michael Moulton	Principal Member of Technical Staff, Advanced Weapon Systems	Sandia National Laboratories
Don Peterson	Design Engineer	Federal Highway Administration, Washington Division
Jeff Phillips	Emergency Operations Specialist	New Mexico Department of Public Safety, Office of Emergency Services and Security
Mitch Pope	Technology Infrastructure Management Section Director	Texas Department of Transportation, Information Systems Division
David A. Price	Program Manager for Transportation Security	Federal Highway Administration, Office of the Administrator
Mary Lou Ralls	Director, Bridge Division	Texas Department of Transportation
Stephen C. Roehrig	Deputy Director, Security Systems and Technology Center	Sandia National Laboratories, Operated for the United States Department of Energy
Shelley J. Row	Director	Federal Highway Administration, Office of Transportation Operations

TABLE A-1: PROFESSIONALS INTERVIEWED AS PART OF THE JULY 3, 2002 DEMONSTRATION OF THE ITA SYSTEM

NAME	TITLE	ORGANIZATION
Thomas E. Rummel	Senior Bridge Project Manager	Texas Department of Transportation, Bridge Division
Bob Seyvani	Field Engineering	Texas Department of Transportation, Maintenance Division
Terry Simmonds	Emergency Management Program Manager	Washington State Department of Transportation
Chuck Slocter	IS Technology Master II	New Mexico State Highway and Transportation Department
Sid Stecker	Statewide Transportation Planner	Federal Highway Administration, Washington Division
Mike Stephenson	Traffic Operations, Technical Support Engineer	Missouri Department of Transportation
Scott B. Stotlemeyer	Technical Support Engineer, Maintenance Operations	Missouri Department of Transportation
Rick Vecera	Office of Liaison, Statewide Operations Center	Maryland State Police, Field Operations Bureau
Todd Walters	Intermediate Information Specialist	Missouri Department of Transportation
Zane L. Webb	Director, Maintenance Division	Texas Department of Transportation
Michael Zezeski	Director, Office of CHART and ITS Development	Maryland State Highway Administration

COMMUNICATION AND ANALYTICAL FUNCTIONS

It is important to recognize that the current ITA system addresses two primary emergency planning and response requirements:

- ❒ communication among stakeholders; and
- ❒ analytical evaluation of available data.

COMMUNICATION FUNCTION

Demonstration of the ITA system on July 3 was primarily designed to prove that communication in real-time over a secure path could be accomplished with existing

technology without the need to expend significant amounts of money at the workstation sites for hardware, software, encryption, telephone, Internet access, and other related communication equipment. The equipment capitalization costs at each ITA system workstation were approximately $5,000. A rendition of the ITA system's basic communication screen is illustrated. The system's ability to satisfy this goal during the demonstration is discussed in greater detail in the next major subsection.

ANALYTICAL CAPABILITIES FUNCTION

The remaining analytical capabilities of the ITA system were not demonstrated because they are not currently fully functional and their ability to be developed to an operational status will most likely require a significant amount of future funding and calendar time. The demonstrated system simply included these analytical concepts such as the status bull's eye and event cone as place markers within the overall system. The developers of the ITA system believe that the data received, via the communication function, can be warehoused and mined so that hypotheses regarding potential terroristic events or scheduled terroristic events can be formulated and tested. One goal is for the ITA system to forecast when a terrorism event will happen if federal, state and local government interdiction does not occur. Another is to be able to establish when and how interdiction can best be achieved so that prevention or substantial mitigation can result.

These analytical functions may require technical equipment capabilities that do not currently exist. This is not assumed to be a barrier, since the first step in the further development phase will be to generate the functional requirements for the communication and analytical components of the ITA system. Since technological development moves at such a rapid pace, it would be foolish to restrict the development of the functional requirements to merely what can currently be supported.

ITA SYSTEM—DEMONSTRATION OF THE CORE COMPETENCIES

The full demonstration of the ITA system was scheduled to begin at 10:05 A.M., Eastern Daylight Time on Wednesday, July 3, 2002. Evaluation of the ITA system required a McCormick Taylor Research Team member to be present at the most important location in every state (and Washington, DC) in which the ITA system was to be demonstrated. These were:

- ❒ the United States Department of Transportation (US DOT), Transportation Information and Operations Center (TIOC), in the District of Columbia;
- ❒ Maryland State Highway Administration and Department of Transportation (MDOT), in Hanover, Maryland;
- ❒ Texas Department of Transportation (TXDOT), in Austin, Texas;
- ❒ Washington State Department of Transportation (WSDOT), in Olympia, Washington;
- ❒ Missouri Department of Transportation (MoDOT) in Jefferson City, Missouri; and
- ❒ the New Mexico Emergency Management Center (NMEMC) in Santa Fe, New Mexico.

The ITA system was also simultaneously demonstrated on July 3 during a dry run at the Federal Bureau of Investigation (FBI), National Infrastructure Protection Center (FBI-

NIPC) in Washington, DC; United States Department of Transportation, Federal Highway Administration (FHWA) District Office in Texas; New Mexico State Highway and Transportation Department (NMSHTD) General Office; the FHWA District Office in New Mexico, NMSHTD District Six in Grants/Milan, New Mexico; the Albuquerque Call Center site at the New Mexico State Police (NMSP); and the Albuquerque Field office of the FBI. McCormick Taylor Research Team members were not physically present in these locations.

As identified by the ITA system developers, the four key communication competencies intended to be proven in concept were:

- ITA Call Center;
- ITA secure messaging, alerts, and warnings;
- ITA secure website; and
- ITA user data analysis/GIS interface.

A scripted scenario, spanning just short of two hours in real time, was the method used to establish these aspects of the ITA system. During this scenario, a mock terrorist plot was to be uncovered from the simple beginning of a traffic accident on the Baltimore-Washington Parkway in Maryland. As the accident is first reported into the ITA system via the call center, by means of a cell phone contact made by an MDOT maintenance crew member and subsequently investigated by the Maryland State Police, those operating ITA system workstations in different locations take a series of actions. These begin with recording the incoming cell phone call and sending a message via the ITA secure messaging system to US DOT and the FBI-NIPC. The original cell phone message, recorded by the ITA Call Center system, is eventually sent to all ITA users on-line, demonstrating an attribute of the Call Center portion of the ITA system. Messages travel as well from the US DOT to the FBI requesting changes to several of the participating states' security alert levels.

The scenario was effective in providing the ITA system the opportunity to demonstrate its core communication competencies. The initial cell phone contact required the system to record the call. MDOT was then to forward the digital wav file of this initial call to all other ITA workstations. There were numerous requirements in the demonstration scenario for participating sites to either send or receive secure messages. Changes were made at prescribed times to the alert levels on the nationwide map on the secure website, including demonstrating certain unique features, such as cross-hatched color coding to indicate that states had received the messages and were prepared for their part in the terrorist interdiction.

As called for in the script, MDOT received the cell phone call that started the scenario and was able to pass it on to most other sites in a form which could be accessed and heard. For almost all sites observed, at least some level of connectivity was verified with other ITA sites. Again, for most of the ITA sites, the secure website was observable together with the changes of security alert color and effect in the desired states. Lastly, by accessing the user data analysis or GIS interface, it was possible to view the highway department databases (e.g., stockpiles) and other data entered for NMSHTD District Six.

In the judgment of the **McCormick Taylor Research Team**, the current version of the ITA system demonstrated the minimum core communication competencies desired and claimed before the demonstration, in a limited application. At least, some ITA sites performed flawlessly.

The ability of the ITA system to act reliably in a sustained manner has not yet been proven. It should be noted that reliability and sustainability issues are technical concerns that can be expected to be resolved in the future and were not targeted competency areas. Unfortunately, the reliability and sustainability attributes were troublesome enough to distract some observers from the fact that the four targeted competencies were established.

At the same time, the **Team** does not wish to overlook the system's apparent current deficiencies and expansion capabilities, much of which is discussed in some detail in the remaining subsections of this appendix. For example, at many sites there were substantial problems associated with the receiving of messages from certain other sites. Some messages were received blank. When first received by the New Mexico Emergency Management Center (EMC), the Call Center wav file could not be either opened or played. For whatever reason, this later changed. At least one message, sent by the New Mexico EMC, did not show up on the secure website under New Mexico's log entries. The stability of the Virtual Private Network (VPN) and the secure website was an issue for many sites.[4] The user data analysis/GIS interface, while successful, was neither a real-time product nor currently linked to the kind of crediting or debiting data warehouse system necessary for true utility in emergency situations.

These latter issues speak, therefore, not to whether the system is competent in the four identified areas, but rather to how its reliability and stability can be increased to the level necessary to sustain use in a realistic, multi-state incident. To this end, the **McCormick Taylor Research Team** makes several suggestions in the following pages related to each of the requisite communication and analytical functional areas. This discussion also identifies and provides information useful to expanding the current capabilities of the ITA system.

FINDINGS FROM THE ITA DEMONSTRATION

A significant number of findings were generated as a result of the evaluation of the ITA system demonstration. They are reported here under the following functional areas:

- ❒ ITA public domain system;
- ❒ ITA virtual private network (VPN) connectivity;
- ❒ ITA connectivity with other management information systems;
- ❒ ITA system details;

[4] This seemed to be primarily related to two factors: insufficient tunnel capacity at Sandia and/or firewall problems at the ITA workstation facilities that disconnected the ITA system, believing it to be a virus or other type of security problem.

- ITA call center notification;
- ITA messaging and website communication protocols;
- ITA user-friendliness;
- ITA user resource databases;
- ITA outreach and training;
- ITA costs; and
- other ITA findings.

ITA PUBLIC DOMAIN SYSTEM

The McCormick Taylor Research Team was advised during its visit to the offices of the New Mexico State Highway and Transportation Department (NMSHTD) on June 26-28, 2002 that the Integrated Transportation Analysis (ITA) system had been developed, up to this point, under a cooperative agreement, primarily between the NMSHTD and Sandia National Laboratories (Sandia), using public funds. Furthermore, it was stated that, as a result, the ITA system would be available as public domain to any requester under the Freedom of Information Act (FOIA).

Currently, only the NMSHTD has ITA up and functioning to a significant degree among its 2,600 employees. Therefore, the availability of the ITA system, under public domain to researchers, students, interested citizens, and evildoers, could generally only negatively impact the security of the NMSHTD data and information. However, if the system is further developed and implemented by an increasing number of states, the federal government and a variety of related entities such as the Federal Bureau of Investigation (FBI) and the local and regional Emergency Management Centers (EMC), the ITA systems public domain status becomes increasingly attractive to terrorists and others interested in disrupting the ability of federal, state, and local governments and other related entities to identify threats, anticipate negative events, and respond to emergency situations in real-time.

During the coordinated demonstration of the ITA system on July 3 in Washington, DC (US Department of Transportation, Transportation Information Operations Center, TIOC) and the states of Maryland, Missouri, New Mexico, Texas and Washington, there were actually 13 ITA connected workstations participating. These included two FBI locations, two Federal Highway Administration (FHWA) offices, an emergency management center, and an NMSHTD district office. It was important during the demonstration to include all of these entities, since they represented many of the agencies that would be part of the potential user group for the ITA system. Of course, the 13 participating locations do not necessarily represent all of the potential ITA users that could be expected to sign on in the event the system is adopted nationally. If that were the case, one could suggest that, in each state, the minimum number of ITA workstations could be approximately 18.[5] By including all

[5] This assumes 8 state DOT regional offices, the state DOT headquarters, 3 emergency management centers, an FBI office, and five other entities of interest. This number may be low on the average if the ITA system becomes adopted with enthusiasm across the country. As such the actual number of ITA workstations could be easily over 1,000. However the base estimate offers a foundation from which the discussion can be developed.

states, there could be approximately 900 potential users. All of these users would appeal to individuals and groups interested in negatively impacting the United States.

One of the intents of the ITA system is to include significant information databases. Such databases may include the listings of all DOT personnel names and titles and the location and number of vehicle fleet and material inventories. With the ITA system available as public domain software, the ability to break into some, many, or all of the local users ITA workstations is increased. Thus, the accuracy of the available data may not be maintainable prior to or during an emergency situation; the exact time when the accuracy of the data is necessary to be dependable.

Of course, having the ITA software system in one's possession does not automatically establish entry into the Virtual Private Network (VPN) used by the ITA workstation, or the ITA web site. Both are accessible through the use of a password system. The NMSHTD representatives indicated to the evaluation team that the password design was thoroughly tested and, after extensive attempts to identify the password using the most sophisticated code breaking software, only a few of the multiple digits were able to be identified after a few days of analysis. This is rather heartening.

However, this does not guarantee that an individual or organization intent on disrupting the well-being of the US and its citizens would not be able to identify a password, which would provide access to the ITA system. It is even more probable that this would occur when 900 or more workstations, each with their own password, are functioning. In addition, with 900 or more passwords being used, the probability of someone being able to simply capture a password from the personnel effects of an ITA workstation operator is nontrivial.

If an unauthorized individual gains access to the ITA system, they would have the ability to create chaos, particularly during a terrorism event, by inputting incorrect messages that would be distributed as fact to all 900 plus system users. Or they would have the ability to understand in real-time and anonymously the steps being taken by local and national law enforcement representatives to respond to an implemented incident. This would allow their organizations to readily counter law enforcement actions as they occur. This would be particularly useful in a multiple-event terrorism activity. Initial activities could be used as a diversion to cause mobilization of emergency preparedness and response personnel and equipment to arrive at a destination that would be further exploited with a poisonous gas or a large explosive charge. Then, the primary target could be attacked with impunity.

The ability to hack into the ITA system (or any other similar system) is a substantial concern under any and all circumstances and has to be adequately addressed. Providing copies of the ITA software system, its user manuals and other relevant information to anyone who asks for it provides the opportunity for evildoers to more fully understand the functionality of the system before gaining direct access to the VPN via password breach.

It is strongly recommended that the current and future versions of the ITA system be placed in an access status that prevents them from being requested and made available as public domain information. This is a very high priority recommendation.

ITA VIRTUAL PRIVATE NETWORK (VPN) CONNECTIVITY

In response to the events of September 11, and in support of the nation's continuing war on terrorism, the ITA system has been rapidly developed and deployed. In creating this valuable resource, system design has largely focused on leveraging existing technological capabilities to meet the heightened threat environment.

The immediate need for ITA's functionality took precedence over the traditional and often time-consuming protocols required to establish long-term, centralized network management capabilities within US DOT, with another transportation agency, or with a third-party vendor. The ITA system currently utilizes a Virtual Private Network (VPN), managed through Sandia, building on an existing research partnership with NMSHTD.

During the July 1 testing and July 3 demonstration process, the VPN connection was the least reliable component of the system at several sites. Slow and inconsistent VPN connections raised issues regarding the need for a more robust connection infrastructure to sustain the ITA system. Of course, ITA's secure network server and client software were configured to demonstrate the feasibility and importance of the system's operational concepts, which was accomplished. The objective was not to deploy a perfect VPN.

However, having achieved the July 3 demonstration goals, the system's further development must necessarily address the need for reliable and sustainable network connections. Namely, the VPN configuration must be enhanced to provide reliable and robust service to a growing and complex user community.

The selection of VPN technology as the backbone of the secure network was a forward-thinking design decision. VPNs are readily scalable. The Department of Justice's Regional Information Sharing System (RISS) provides an example of the fully expanded capability of VPN technology to support secure communications. This system uses VPN protocols to enable law enforcement officers from more than 5,000 state, local, and federal agencies to securely access criminal intelligence databases.

The ITA's mission is to connect State DOTs (both internally at the district or division level and externally with each other) to regional and federal offices of FHWA, FMCSA, FBI, the emerging DHS organization, as well as State EOCs, State Police and National Guard units, and major municipal traffic management centers; the fully expanded ITA system could eventually number users in the thousands (prior to later-stage development emphasizing connectivity to other critical infrastructures).

To achieve this level of network access, functional requirements for designing an effective VPN solution must be identified. A VPN strategy, critical to the next phase of ITA system development, must address the following issues.

- ❒ Identification of the organization that will assume full-time VPN administrator functions. In the months to come, administration of the VPN will require considerably expanded resources as more users come online. The options are to

maintain this function with Sandia/NMSHTD or to migrate it to the US DOT, another governmental or pseudo-governmental agency, or a secure third-party contractor.

- ❒ Identification of the organization responsible for providing VPN trouble-shooting support for the user community. To date, the NMSHTD has made considerable personnel and other investments in addressing these issues. The current VPN relies on the user's existing Internet Service Provider (ISP)/Local Area Network (LAN) to accept ITA software and an authenticated connection to a secure network server to create a virtual circuit for moving secure data and to disable other ISP/LAN functions. In this configuration, compatibility among and between ISP/LAN protocols is expected to become more of an issue, which could expand exponentially in complexity with additional users. Options for the financing, staffing, and budgeting of this function need to be identified and evaluated before an ultimate decision can be made.

- ❒ Determination of the need to migrate the VPN connection protocol from the current platform to an exclusively network-based system. ITA currently requires Cisco VPN Client Software to be installed on a stand-alone computer-processing unit (CPU) connected to the user's LAN. Migration to an exclusive network-based protocol would eliminate the need for the CPU, and may expand the accessibility of the VPN to more workstation users.

- ❒ Creation of a reliable and private tunnel for secure communications using encryption and authentication functions so that local Internet/ISP configuration issues can be resolved as more and more networks are integrated into the system. Methods of encryption, and other security practices involved in VPNs, will have to be tested to ensure their effectiveness and integration across the range of possible products. Alternatively, the functional requirements for hardware and software, communication, networks, and other components would have to be developed so that all ITA workstations have the same equipment and software and can consequently avoid the issues of compatibility, reliability, and sustainability.

- ❒ Determination as to whether a set of regional centers will be needed to manage the traffic generated by full-scale implementation of the ITA system. The configuration of such centers would have to be addressed. During the demonstration, participating State DOTs emphasized the significance of regional relationships.

- ❒ Appropriately distributed VPN centers may also provide opportunities to identify and link users who play an important role in the protection of a specific region. Many users may not be significant to other regions or the nation.

- ❒ Determination as to whether there will be additional user authentication requirements at some sites, dictated as a result of the large number of potential users, with varying degrees of need and on-site physical security capabilities (for example, a smart card and ITA client verification software on the workstation).

- ❒ Determination of the need to have varying levels of access associated with users of the components within the ITA system, which ultimately creates the need for layers of authenticity and user passwords. For example, state law enforcement may have different needs from DOT traffic management centers, even if a single ITA workstation is shared at a coextensive facility.

- ❒ Development of protocols for the expansion of the ITA website to include links and additional connectivity while maintaining the necessary security capabilities.[6] A companion is determination of protocols for interfacing the ITA system with other secure and non-secure sites.

- ❒ Development of functional requirements that cause the ITA system to self-monitor daily usage of the operator(s) to ensure system use is as designed.

- ❒ Development of protocols and capabilities to address intermittent service failures, particularly since the connection to the VPN is only as reliable as the ISP/LAN.

- ❒ Development of a management function designed to address and process requests for connectivity based on predefined rules concerning the type and needs of the user.

- ❒ Determination of the ITA system's requirements regarding transmission options for redundant network connections.[7] VPNs have been plagued by questions of reliability because they often are dependent on the Internet and its inherent bottlenecks. This situation may be exacerbated in a regional or national emergency.

- ❒ Determination of the functional requirements for bandwidth and upload/download rates associated with VPNs since access speeds will never surpass the capability of the ISP.

- ❒ Incorporation of the needs associated with increasingly band hungry attachments, such as video feeds from traffic management centers and secure video-conferencing capabilities into the functional requirements.

ITA CONNECTIVITY WITH OTHER MANAGEMENT INFORMATION SYSTEMS

The GIS U/R function demonstrated for NMSHTD District 6 was successfully evaluated during the July 3 demonstration. State DOTs also indicated their interest in using ITA to connect to high-powered digital networks available (or under development) to support incident planning, training, and exercising, as well as incident management and response. Several state representatives commented that vendors of other state or Federal agencies, with advanced incident management systems that could be tailored to address State DOT needs, had approached them.

---

[6] This is further addressed in the subsection below on the connectivity of the ITA system with other management information systems.

[7] Fiber, satellite, digital subscriber line (DSL) and asymmetric digital subscriber lines (ADSL), or cable.

To ensure its primacy among threat and consequence management networks, the ITA system should be capable of providing connectivity to other key infrastructure protection and incident management systems. This connectivity would support the use of the ITA system for security-related threats and incidents in addition to managing emergencies, natural disasters, and hazardous materials incidents. By promoting genuine all hazards management for State DOTs and other transportation operators, the ITA system would dramatically increase its value as an essential resource. This is a stated objective of the ITA system.

Based on the results of the July 3 demonstration, and independent research conducted by the **McCormick Taylor Research Team**, the following networks/systems appear to offer the greatest user benefits for interfacing with the ITA system:

- ❒ United States Department of Transportation, Activation Information Management (AIM) System;
- ❒ U.S. Marine Corps Systems Command, Consequence Management Interoperability Services, Incorporated (CMI-Inc);
- ❒ Defense Threat Reduction Agency, Consequence Assessment Tool Set (CATS); and
- ❒ Federal Bureau of Investigation, National Infrastructure Protection Center, InfraGard.

Each of these systems is briefly described below.

US DOT's Activation Information Management (AIM) System

This is a web-based emergency management system used to gather, update, and disseminate essential elements of information (EEI) related to transportation emergency situations. It was designed to allow US DOT headquarters and regional personnel to report and display the status of the nation's transportation systems and provide senior decision makers with a nationwide situational awareness. AIM has a mapping component and contains several types of reports, including the following:

- ❒ event;
- ❒ incident;
- ❒ facility;
- ❒ situation;
- ❒ duty log;
- ❒ mission critical; and
- ❒ FHWA alert bulletin.

This system is currently only accessible to US DOT personnel. Additional information is available from Ms. Gale Hines, 202 366 5118, gale.hines@rspa.dot.gov and at http://www.rspa.dot.gov/oet/activation_info.html.

Consequence Management Interoperability Services (CMI-Services)

The CMI-Services system offers extensive GIS mapping and modeling capabilities for threat management and incident response. Its primary focus is providing the consequence management community with the ability to effectively share digital information. While still under development, this system is expected to have a highly effective approach to coordinating the needs of multiple users involved in incident response. Development of this network has been closely coordinated with the Department of Homeland Security (DHS). Significant research has been completed on the needs of first responders in municipalities, state governments, and emergency organizations, along with defense and civil agencies of the federal government that may be beneficial to the ITA system. CMI-Services has developed an innovative approach allowing multiple users at a local level to map and manage critical incident response, share edits and revisions to operational plans, and post final versions to the secure site.

The CMI-Services team consists of a core group that works in a dedicated integrated manner and a collaborating group that includes specialized efforts by a number of organizations. The core group consists of approximately 40 full-time staff members drawn from Battelle, MTS Technologies, Inc., and Veridian. Obviously, the resources assigned to this effort are massive compared to the bootstrap efforts of the NMSHTD on the ITA system. Yet, the ITA system has been able to demonstrate significant existing competencies in addition to identifying innovative and far-reaching analytical concepts. The CMI-Services team is located in Garrisonville, Virginia. Collaborating partners include SRA, Sverdrup, Teledyne Brown Engineering, Public Safety Systems, Inc., Georgia Tech Research Institute, the Memorial Institute for the Prevention of Terrorism, the Chemical/Biological Information and Analysis Center, and Emergency Information Interoperability. Additional information on this system is available from Mr. Doug Bryce, 703 784 5897 and at http://www.cmi-services.org.

Consequence Assessment Tool Set (CATS)

This system was developed for the Defense Threat Reduction Agency (DTRA) and the Federal Emergency Management Agency (FEMA). The Consequence Assessment Tool Set (CATS) is available to federal, state, and local government emergency response organizations nationwide. CATS assesses the consequences of technological and natural disasters to population, resources, and infrastructure. Hazards addressed by CATS range from natural disasters, such as hurricanes and earthquakes, to technological disasters such as industrial accidents, terrorism, and acts of war.

CATS combines state-of-the-art hazard and consequence prediction, digital databases and a geographic information system (GIS) within a graphical user interface (GUI). CATS provides significant assistance in emergency managers' training exercises, contingency planning, logistical planning and in calculating requirements for humanitarian aid. Information on CATS is available from the Consequence Assessment Branch, Defense Threat Reduction Agency, 703 325 6106, acehelp@dtc.mil and at http://www.dtra.mil/td/acecenter/td_cats.htm.

FBI InfraGard System

The FBI InfraGard System is currently the nation's most advanced threat and warning system, with more than 4,000 subscribers. InfraGard provides four basic services to members: secure and public websites; an alert and incident reporting network; local chapter activities; and a help desk.

Under this program, the FBI provides a secure electronic communications capability, so that the NIPC can provide threat information to private industry owners and operators, and encourage private industry coordination with law enforcement, and each other, on cyber and related physical incidents. Since getting online in 1998, InfraGard has received thousands of threat reports and has posted more than 100 warning advisories and alerts to subscribers. Local chapters, coordinated through each FBI field office, have proved to be an effective way to solicit coordination with the program and to support industry efforts to connect with and use the network. InfraGard also supports the FBI's Awareness of National Security Issues and Response (ANSIR) Program and Key Asset Program. Information on this system is available at http://www.infraguard.net, and at http://www.infraguard.net/fieldoffice.htm.

Through NIPC, state and municipal governments are being encouraged to develop threat, warning, and incident management networks for their critical infrastructures. The Texas Infrastructure Protection Center (TIPC) is the most sophisticated of these systems currently under development. More information on TIPC, including a detailed report on the network's functionality and requirements, is available at http://www.oag.state.tx.us/sipac/sipac_toc.htm.

ITA SYSTEM DETAILS

Utilization of the ITA system can be expected to occur in a variety of ways. It seems clear that an initial capitalization and installation cost of $5,000 per workstation[8] is certainly affordable to all states and to most other agencies interested in the capability. However, in the aggregate as more and more entities are added to the ITA network, the combined startup costs become substantial. These initiation fees associated with joining the fraternity are reasonably minimal compared to the operating costs associated with personnel coverage and maintenance of the necessary databases. In addition, the costs associated with data mining and other more advanced functions have yet to be addressed.

Secretary Pete Rahn of the NMSHTD insisted, during a meeting on June 27 in New Mexico, that the ITA system, partially developed by the NMSHTD's Research Bureau, will be useful for the annual fire fighting and winter weather seasons as well as the less likely (and

[8] The standard ITA system hardware package includes: two PC servers with 100 GHz memory and 1.7 GHz processor; one monitor (a standard 17-inch monitor is assumed, but for maximum observable functionality a larger screen would be more desirable); one mouse; one KVM switch (keyboard, video, mouse); one incoming telephone line; one headset; two speakers; and two power strips. Additionally, each site must have the following equipment: two analog phone lines with phone numbers; 110 volt electrical power; Internet access, and a data line to the LAN.

presumably less frequent) possibility of dealing with terrorist incidents. This type of imperative for the ITA system, to be useful in a variety of emergency situations, is actually a plus for its ultimate build out and implementation. Multiplexing the functionality across many of the capital, maintenance, and operating costs suggests an efficient amortization that will impress decision makers. It seems likely that, if the ITA system is to have true functionality for the states, it must have applicability for more than simply terrorist incidents.

In states more compact than New Mexico, with higher concentrations of traffic and people, the application of the ITA system may be very different. It was suggested that, in Maryland, for instance, emergency operations and traffic management are already coordinated and supervised in a very sophisticated way. There may be less need for the ITA Call Center function, as calls are currently routed satisfactorily in other ways to the most appropriate decision maker with access to resources. A state like Maryland might be more interested in accessing the ITA system for its messaging capabilities rather than the Call Center function.

This speaks to the need for flexibility in the way that the ITA system is ultimately configured. As the system must be accepted on a state-by-state basis as part of an integrated national transportation protection system, the ITA system will need to be tailored to the individual needs of the participating states. It appears that the ITA system developers have already anticipated having to make custom fits in many instances.

If the ITA system becomes part of a national, secure communication and analytical network, there will have to be national messaging protocols and acceptance of a common (or at least comprehensible) set of terms (jargon) for transportation elements. For instance, in New Mexico, highway maintenance facilities are called patrol yards whereas, in many states, patrol is a term reserved for the state police. In order to develop a true national network, there will have to be standard elements of the system that remain unchanged from state-to-state in order to allow uniform programming updates and unimpeded connectivity among the states and US DOT. This is an extremely important issue since it will ultimately be the responsibility of one entity to keep the ITA system current and fully available for use.

A question also arises as to the initial source of information into the ITA call system. In New Mexico, as a start, wallet cards were issued to every one of the 2,600 NMSHTD employees. Each contains a telephone number for the ITA statewide call center, which is manned by the New Mexico State Police. The decision was made to not make the call toll-free, a subject of some controversy, but intended to help ensure that calls made were needed and legitimate. All of these eyes and ears concerned with security and safety issues seem like a substantial number; but given the enormous amount of highway assets (11,400 miles of state roadways) to cover in a state the size of New Mexico, it is reasonable to suggest that it would be worthwhile to expand the field network beyond the state's highway and transportation department employees. The next steps might well be to include municipal and local highway maintenance workers

or other state employees and eventually perhaps, members of the general public, such as the operators of private motor carriers.[9]

The consequences of each of these enlarged circles of possible contacts are obvious; it provides access to the ITA system by those who are less knowledgeable about what truly constitutes an unusual or suspicious circumstance. If ITA calls begin to come in from, for instance, private and for-hire truck operators, there will be more points of observation for anything unusual happening on the state's roadways. However, there will almost certainly be more calls overall and the number of unproductive and unimportant calls will likely rise.

As the system is currently functioning, more points of uncontrolled observation almost necessarily translate into a need for more attention to the staffing of the ITA system call centers and the day-to-day maintenance and upkeep of the databases and software. It also increases the data warehousing and data mining requirements, and the need to establish protocols for the identification and disposal of non-valuable information.

It has been suggested that the ITA system only makes sense when staffed 24 hours per day, seven days per week (24/7). This is unlikely to occur at many workstations and even more unlikely if the ITA system continues to be a stand-alone program[10], which although undesirable, seems probable due to security implications.

Emergency operations centers (EOCs) within many states and regions are typically not staffed on a 24/7 basis. Rather, as an emergency situation develops, the relevant EOC is usually staffed-up. While there is often some skeleton staff available at all times to step in, EOC staffs are not generally assigned on an around-the-clock basis.

During the demonstration, there were frequent questions about who would be sitting at the ITA system workstations. There is a concern among members of the law enforcement and security communities that the current ITA system is not secure enough to be able to communicate truly sensitive information. The concept of having all ITA system workstation operators possess a security clearance may be important to get the security community to be more comfortable. However, it increases the difficulty of getting a maximum number of the states and other entities to sign on to the ITA system network.

ITA CALL CENTER AND NOTIFICATION

This element of the subsection analyzes the ITA call center capabilities and system notification protocols associated with these capabilities.

---

[9] The Federal Motor Carrier Safety Administration (FMCSA) recently announced that private trucking companies had been asked to instruct their vehicle operators to be on the lookout (BOLO) for unusual circumstances during their travels. This is an important concept since 1,000s of truck operators are traveling almost all of the nation's primary roadways on a daily basis. These eyes and ears need to have the ability to convey collected information to a focal location which in turn can pass it on up to the ITA call center for input and evaluation. Thus, establishment of relationships with all of the major trucking firms is a necessary activity. Provision of a toll-free number, that accesses the ITA call center, would facilitate communication more effectively.

[10] Integration with other systems would increase the value of the ITA system to the users of those systems.

Features of the ITA Call Center

Many demonstration participants seemed impressed with the technology associated with the ITA system call center. They also had many suggestions for improvement concerning the initial contacting of the state DOT or agency and the continuous communication of threats to those agencies responsible for housing the ITA system.

Initial Contact at the ITA Call Center

Many interviewees were impressed with the ITA software system's ability to record the initial telephone call from the event scene and forward that exact wav file, or sound bite, to key responders. They were also impressed with the system's email-like capabilities to forward photographs, in PDF format, to decision makers with a need to know. During the July 3 ITA system demonstration, at the Maryland State Highway Administration of the Department of Transportation (MDOT), an initial cellular telephone call was received by the ITA system administrator. The message was recorded and played back for the observers to hear first-hand. A few moments later, a PDF file was received through the ITA system. It was a picture of the actual scene. This initial, first-hand contact with decision makers is just one of the significant features of the ITA system that was 100% functional. Unfortunately, some state DOTs involved in the demonstration did not have as valuable an experience with the initial call center capabilities. The following problems could occur but should be prevented by enhancing the ITA system via a set of functional requirements:

- ❒ wav files or PDF files may not be available or may not open during a real crisis;
- ❒ nomenclature or definitions may vary among states;
- ❒ incoming messages may be difficult to decipher;
- ❒ specific state DOTs may have other systems already in use for threat notification that may conflict with the ITA software system;
- ❒ some agencies may not be able to receive calls from an automated system or they may require priority user codes for access;
- ❒ the Virtual Private Network (VPN), a security function of the ITA software system, could drop off at any time, even during the initial contact phase;
- ❒ many initial contacts on the safety and security lists may not be available, which could delay the processing of a critical message; and
- ❒ some agencies may require several different call lists (in addition to the safety and security lists) to be activated simultaneously, immediately following the initial call into the ITA software system.[11]

[11] This causes additional problems as follows: two or more call tree professionals may try to respond to a message at the same time creating excessive demands to the system; or a very low level decision maker returns the activation call prior to a much more knowledgeable professional, and makes an incorrect assessment of the situation, despite the fact that the more experienced professional is truly available, but locked out. If both respond and their directions are posted, which is to be implemented? How do reviewers of the communication messages know what is actually being implemented?

ITA Call Center Improvements

During debriefing discussions, some additional suggestions were made regarding solutions to the problems listed above. Many questions were also raised that may be beneficial to the further development of the ITA system. Many respondents feel that the true success of the demonstration of the system is the dialogue occurring regarding a secure communication infrastructure. The following suggestions may be beneficial to continuing this discussion and ultimately improving the call center and notification functions.

ITA Website

ITA workstation operators should be trained to simultaneously use the ITA website in conjunction with the ITA system. The ITA website should be truly secure so that all information coming into the ITA call center can be simultaneously posted (including sound or wav files and PDF formatted photographs). Using the website will help integrate the ITA system with existing management information systems already in use at various agencies. Having a website icon available on workstation desktops would allow some users to rely on other systems already in place while having access to ITA system information when it is identified as important. Also, real-time access via the ITA website may be beneficial to some agencies requiring access to the system from remote locations. In the extreme event that DOT or agency personnel in a command center with the ITA system workstation need to relocate to a secondary or tertiary command center, accessing the ITA system information via the Internet could be very advantageous. Additionally, if the call center function of the ITA system is not being utilized by a particular agency, the information originally received will still be posted on the ITA website for that agency to easily access.

The website must be absolutely secure. ITA system developers need to clearly put themselves in the shoes of hackers, so that all necessary and appropriate firewalls can be identified, developed, installed, modified as necessary, and maintained. Potential ITA system users are concerned about the risk of posting timely national security information on the World Wide Web.

ITA Call Center Integration

The ITA system should provide a plug-and-play capability with other systems already in existence and being used at state DOTs and other various agencies. For example, the New Mexico Emergency Operations Center (EOC) is willing to use the ITA system, as long as the call center function is accessible remotely and can receive initial contact messages via the pages of key personnel. Some potential users of the ITA system are interested in using all of the communication and other functions except the call center. They may want to use other devices, while still having access to the ITA system for communicating with other states and other agencies. They should also be able to acquire threat information from other notification sources and then use the ITA system to forward messages and keep in contact with other agencies.

ITA Call Center Differentiation

The call center should be able to differentiate specific calls as a primary function. Many responders mentioned that adding a caller ID function to the ITA system would be beneficial (see more on this below in the subsection titled ITA Call Center Data Mining). Interviewees were impressed with the ITA system's ability to differentiate a safety-related call from a security-related call; however, the ITA system should also be able to notify additional call lists simultaneously. The Washington State DOT thought that the ITA call center could be strengthened by adding a broadcast function that would route automated call lists to a phone bank or alphanumeric paging system for immediate notification of an entire call list related to a specific threat. If the ITA call center function could initiate this immediate notification, instead of contacting security or safety personnel one by one using a single call out line, this would allow for near real-time communication of specific threats to key decision makers.

The ITA Call Center and Law Enforcement Agencies

Some state DOTs felt that they should not be held completely responsible for receiving the initial calls or essentially housing the ITA system, despite the fact that it was primarily designed to support them. Some state DOTs wanted to include law enforcement agencies on initial call center contact lists and require certain law enforcement agencies to house ITA system workstations, in addition to the workstations in place at transportation agency facilities. This is a concept that merits additional evaluation.

ITA Call Center Availability

Call center operators should be available to receive calls on a 24/7 basis. Some state DOTs suggested that, if messages can be forwarded directly from the ITA system to Nextel or other paging system devices, perhaps this would eliminate the need for operators to be available on a 24/7 basis. However, most agencies felt that the system needed to be monitored, for security reasons, on a 24/7 basis by trusted and trained operators. Operators add a human aspect to the ITA call center and allow those in distress to talk to a real person. Also, round-the-clock employees, such as technicians, should be available to assess how the ITA system is operating from the initial call to the deployment of a response plan. Requiring personnel to be available 24/7 is a way to assure the effectiveness of the ITA system.

ITA Call Center Protocols

Much of the discussion above addresses issues dealing with specific protocols of how the ITA system will operate.

- ❒ Who will be called first?
- ❒ How will they be contacted?
- ❒ Does every agency need to be notified in the same or similar way via the ITA call center and notification functions?

Figure A-1 outlines the ITA call center protocols observed during the July 3 demonstration. It also assesses the performance of the ITA call center and notification functions and shows that these protocols were completely satisfied. Additional research and study is expected to result in the identification of additional items for this list. This checklist is designed to provide ITA developers with a rubric for training operators to follow protocols, and to aid with the development of new ITA call center protocols.

ITA Call Center Data Mining

The concept of data mining is also addressed in other subsections of this appendix. However, the ITA call center and notification functions are a good place to focus. A common suggestion among state DOT personnel and other officials is to allow the ITA call center to trace calls through a caller identification system. This will help to determine location, nature of threat, validity, and other facets of the call. This information can then be placed in a database for analysis. The ITA system should possess the functionality of determining if patterns exist among the data, so that threats can be predicted, and ultimately prevented or mitigated. Examples of information that can be analyzed through a data mining or patterning process are listed below:

- ❒ key words used (e.g., bomb, truck, spill, etc.);
- ❒ locations (determining patterns can be useful to prevention when predicting future locations of attacks);
- ❒ nature of threats (if states are reporting similar threats, perhaps a coordinated attack is underway and can be prevented or mitigated);
- ❒ content of calls;
- ❒ percentage of real threat calls versus invalid or phony calls;
- ❒ phone numbers that call in to the ITA software system (which can be added to a contact list so that follow up information can be gathered); and
- ❒ many others that can be developed as the result of future research on functional requirements.

The ITA system should contain analytical tools for gathering and data mining call center information to determine patterns that can be used to prevent harm. The call center and notification functions provide important interfaces that facilitate the process of connecting agencies to the ITA.

ITA MESSAGING & WEBSITE COMMUNICATION PROTOCOLS

This subsection focuses on the website and messaging components of the ITA system and presents recommendations based on assessments by participants and observers in the July 3 demonstration. It does not detail technological assessments; rather it recommends steps toward policy development that are necessary to support future ITA development and deployment. The subsection is organized to address the

FIGURE A-1: ITA CALL CENTER PROTOCOLS DEMONSTRATED ON JULY 3

PROTOCOLS	Demonstrated on July 3, 2002
Create call list by clicking on the Contacts button on the call center main screen.	✔
Identify contact by name, company, title and three telephone numbers (work, home and mobile).	✔
Create and use password for each contact to ensure receipt of message.	✔
Initiate call list by clicking on the Call List button on the call center main screen.	✔
Create separate call lists for security incidents, safety incidents and incidents likely to require no additional action.	✔
Operator to receive emergency calls from ITA call center number.	✔
Operator to enter information into distinct fields regarding caller information.	✔
Operator to enter information into distinct fields regarding caller incident description.	✔
ITA software system to record incident call.	✔
Operator to click on Call List button to initiate call list.	✔
Operator to track call list execution and status.	✔
ITA system to ask operator if law enforcement has been notified.	✔
ITA system to log and store operator report.	✔
Operator to review recorded messages.	✔
Operator to send recorded messages.	✔
Operator to use Call Center tab to update the alert status cone.	✔
ITA system to create greeting for the automated call center function.	✔
ITA system to change greeting on message.	✔
Operator to command ITA system to test greeting function.	✔
Operator to save new greeting on ITA call center.	✔
ITA call center to receive and record calls.	✔
ITA call center to initiate automated call list.	✔
ITA call center to call numbers on contact list.	✔
ITA call center to recognize secure user password.	✔
ITA call center to provide user who entered password with additional notification options.	✔
ITA call center to automatically execute options selected by user who entered password.	✔
Operator to click on Outbound Messages to show who has been called and content of calls.	✔
Operator to click on the Call Log button for further information on the status of phone calls.	✔

effectiveness of the ITA system as it relates to the management of information assurance with regard to:

- ❒ accountability;
- ❒ timeliness;
- ❒ integrity and security;
- ❒ utility; and
- ❒ interoperability.

It is recommended that ITA system policies adhere to these five information assurance principles as they relate to the flow and management of information through the messaging and website functions.

Accountability

Whether the ITA system and its policies, standards, and requirements are overseen by a steering committee of designated representatives or a single entity, it is critical that the system be managed and maintained by and from one central location. The above listed principles require the ITA system to be owned by a single entity to ensure that system policies, procedures, and standards are enforced without being compromised by fragmented decision making authority. Of course, there are levels of decision making that will be necessarily delegated to ensure the utility of the system; however, system-critical operating and information assurance principles should be subordinate to that entity with ultimate decision making authority.

At each ITA system site, the explicit assignment of responsibilities for ownership or oversight of the system itself, inputs and outputs, and interagency coordination requirements should be developed. Governing principles should be consistent with the central ITA entity.

A variety of issues, including the following, need to be addressed.

- ❒ Identification of a governing body to enforce developed ITA system policies, procedures, standards, and requirements.
- ❒ Identification of an entity and location for central server ownership, operation, maintenance, and protection.
- ❒ Requirement of ITA site users to identify a point of contact for the system's administration, security, and maintenance.
- ❒ Development of ITA information-sharing policy agreements for execution among users. Agreements should observe current federal, state, and local government policies, codes or laws regarding the dissemination of sensitive information, as well as governing constraints on federal-to-state and state-to-state accountability and liability.
- ❒ Development of policies that govern and procedures that identify user responsibilities and protocols for notification, acknowledgement, discernment, and tracking of information disseminated through the messaging service.

Timeliness

Information regarding the detection, warning, and response duties for security and emergency incident prevention and management requires an element of timeliness to be

truly effective. Policies must be in place to ensure that the ITA secure messaging and website functions are continuously refreshed and updated to promote timely dissemination of information. During the July 3 demonstration, slow transmission speeds and occasional service interruptions prompted questions regarding the utility of the system if timeliness cannot be ensured.

A variety of issues, including the following, need to be addressed.

- ❒ Identify communications backbone that will support 24/7 operations during all types of disasters and emergencies.
- ❒ Develop performance standards for messaging that require the system and all users to fully satisfy an acceptable minimum transmission speed.
- ❒ Develop a messaging plan to automate responses when possible to support the timeliness of data transmission (e.g., message tags that identify type of action or non-action required and are associated with notification queues).

Integrity and Security

The accuracy, completeness, and reliable transmission and reception of information and its validity are critical to the value of the ITA system. Further, protocols must be in place to protect sensitive information from unauthorized disclosure, electronic penetration, and exploitation. These security measures are not confined to information technology applications or human resources management, but to the system as a whole, including protection from physical exploitation. The July 3 demonstration was held in open forums to facilitate greater size audiences for participation and observation. The integrity of the ITA system, with regard to information security, was presented through discussions with ITA technical representatives prior to the actual demonstration.

A variety of issues, including the following, need to be addressed.

- ❒ Identify interagency sensitivity concerns regarding the dissemination of information, including sanitization, data analysis, and reporting.
- ❒ Identify and track authorized ITA users and sessions.
- ❒ Develop a system security policy that identifies security measures designed to protect the ITA system from both internal and external threats.
- ❒ Develop minimum security standards.
- ❒ Require ITA end users to develop system security plans and procedures that adhere to ITA's system security policies and, at a minimum, address:
    - ○ security management structure and assignment of roles and responsibilities;
    - ○ system/application rules;
    - ○ user account management;
    - ○ general and/or specialized training;
    - ○ personnel controls and security (including hiring and termination);
    - ○ incident response;
    - ○ third party management;
    - ○ continuity of support and/or contingency planning;
    - ○ system interconnectivity and information sharing;

  - facility protection; and
  - threat management.
- ❒ Develop verification standards for evaluation of transmitted data (voice, text, photo).
- ❒ Develop information security risk management plan.
- ❒ Develop change control procedures (changes or updates to hardware, software, firewall, or network management systems).

Utility

The utility of the ITA system will be derived from its ability to earn the confidence of the end user. At a minimum, the ITA system must satisfy its core competencies in a reliable and sustainable manner and achieve this while ensuring that users receive information that is useful and relevant to them, find the system to be reliable and credible, and receive follow-up information on the evolution of a threat to its resolution.

A variety of actions, including the following, need to be taken:

- ❒ Develop policies that direct the flow of information based on relevance to the user.
- ❒ Survey states to identify non-terrorism uses that will support leverage for funding and resource allocation.
- ❒ Develop a plan that clarifies inter- and intra-agency roles and responsibilities for information dissemination.
- ❒ Create a secure discussion group on the website for users to communicate ideas and best practices regarding the system that is separate from the event management site.
- ❒ Develop procedures for the management of ITA system user requests and concerns.
- ❒ Develop management reports to facilitate after action reporting and analysis, ITA technical system feedback, and user activity.

Interoperability

Currently, there are state departments of transportation and other potential end users that have management information systems similar in functionality to ITA. To achieve the greatest utility from the ITA system from the state's perspective, either integration or replacement of current systems must take place or clear procedures must document how the systems will coexist and communicate. Traffic incident management systems, emergency management call centers, and (in the case of public safety agencies) communication centers and dispatching, as well as secure systems for threat dissemination create potential parallel efforts, fragmentation of services, or confusion. The secure messaging and website of the ITA system must be deployed such that it can be incorporated or improve current user operations.

A variety of actions, including the following, need to be taken:

- ❒ Ensure cross-function coordination between the messaging service and the website (integration of key elements).

- ❒ Develop support plans for potential users that help them identify methods of ITA deployment that will leverage funding and support.

ITA USER-FRIENDLINESS

The Missouri Department of Transportation's (MoDOT) technical support engineers and information specialists provided input and recommendations on system capabilities and ease of operation during the communications check and practice demonstration. Their comments were reflective of many of the participants in the demonstration. Major issues regarding the user-friendliness of the ITA system are discussed below.

Terminology Consistency

An immediate concern was the potential confusion due to inconsistent use of terminology and jargon among the states. For example, New Mexico identifies equipment location areas as patrol yards. This term identifies State Police offices in Missouri. Different agencies and departments get comfortable with certain terminology and would find it difficult to change. One solution would be to develop a term convention that would establish a consistent definition for the most commonly utilized 300 words. ITA system operators would be trained to understand the agreed upon definitions and would consistently utilize the terms.

GIS Map and Layers Screen

The color-coded graphic map of the United States should indicate more clearly where there are significant incidents of possible terrorism or emergencies to portray the overall national situation at a glance. The national overlay could have several shape files on such topics as terrorism, floods, earthquakes, hurricanes, forest fires, tornados, sever ice conditions, etc. The ITA system user could select the overlay of interest from a key by clicking. Each specific event or incident could be spatially located on the national map using an icon. Clicking on an icon would provide direct access to an information database that could identify each relevant message event.

When the spatial area is drilled down to the county and township levels, the route numbers and other information, in highly developed or congested urban areas, become obscured. The provider of the GIS mapping should be contacted to determine if clearer versions are available.

The GIS mapping will need to always be the latest possible versions if the ITA system is going to be able to be successfully used to establish alternate traffic routes during emergencies and to assist law enforcement in the closing of roadways, so that a perpetrator can be apprehended. During the demonstration, it was established that the current GIS mapping does not include a number of known bridges. This example is very important since bridges are known to be potential targets for terrorists.

It would also be useful for the available maps to be able to display in real-time the current status of road closures and the traffic conditions associated with the rerouting. This suggests that interfacing the ITA system with intelligent transportation system (ITS) traffic monitoring equipment displays would be useful. This would also facilitate the use of variable message signing units to be used to direct traffic away from the incident site as identified in the ITA system. Such signs may also prove to be of value in controlling the travel direction of perpetrators attempting to flee.

Message Board

The ITA system should be capable of confirming that sent messages and their attachments have been received and opened. One federal reviewer identified the audible message alert as a very positive attribute of the ITA system. However, the message is only repeated once. There should be a greater interval between the initial annunciation and its repeat so that in the event the workstation operator leaves the room there is an improved probability that a missed message will be accessed. This could also be handled by placing an icon or word message on whatever screen is displayed, indicating that a message has been received. This could also display the number of messages that have been received, but not accessed by the workstation operator. These capabilities should be interconnected to a message access tracking function. In the event a received message is not accessed within a certain amount of time, another audible message should be generated. The audible alert would be repeated, perhaps at an ever-increasing degree of loudness, so that the ITA system is persistent in delivering the messages.

There was concern that the ITA system causes the message text to scroll from the current message to the beginning of a new message at the moment it is received. If a flood of messages is received, the workstation operator will have difficulty understanding the incidents and their relationship as a result of incomplete processing of the messages.

The address book should include a heading for “TO” and “CC” similar to email messages.

The ability to pre-type text in the notepad is a desirable feature. It is not apparent whether the ITA system allows text to be cut and pasted.

It was apparent that the ITA system had difficulty sending and receiving longer messages. The length of acceptable messages is unknown. In an ideal world, there should be no limit to the length of sent and received messages. Similarly, the size limitation of attachments should be indicated. This is generally related to the portal size at both the sending and receiving file servers. It is typical for an oversized attachment to not clear the local portal without even receiving a message. Most systems do report back if a message clears the local portal but is excessive in size in relation to the receiving portal. The size of attachments sent and received should be specified to the maximum expected use, plus a contingency. This should be part of the hardware and software specifications for the workstation and local network.

In addition, the sent message indicator should include an acknowledgement that an attachment was included with the message.

The Expand Message button was not clearly visible, during the July 3 demonstration, and the observers had difficulty reading the text. The message dialog box did not include the text that was sent.

Call Center System

The system should be located in a 24/7 environment to be entirely effective. The system should also have the ability to include contacts at the regional level. The state of Missouri would be better served to maintain one system to be utilized by all agencies. This is a specification issue for the national system that needs to be addressed.

Common Screen Features

The ITA system should easily allow each workstation user to quickly move between the software and website so that all information regarding an incident can be reviewed. It is most desirable for:

- ❒ both to be open at the same time;
- ❒ the website to refresh its content each time new information is added; and
- ❒ the functionality to send a message to the workstation operator that he/she needs to replenish the website by clicking the refresh button.

The ITA system workstation screen appeared to refresh at an unspecified interval. This concerned some observers. Perhaps information in the user manual on refreshment rates would dispel these concerns. Ideally, the operator should not have to worry about refreshing the screen, since the system should automatically accomplish this task, according to an accepted and specified protocol.

ITA Event Indicator Cone

The event indicator cone is perhaps the least understood component of the ITA system by users and observers. It is believed that this cone is intended to indicate the posting of alert events. The cone did not appear to function properly or clearly provide information during the demonstration. At best, it seemed to indicate only one event had occurred. It is not clear if the event indicator on the cone was associated with each message or with a series of related messages. As stated in the subsection entitled Communication and Analytical Functions, this is a part of the ITA system that needs extensive research; the existing display serves primarily as a bookmark on the standard ITA status screen and within the system. Thus, considerable attention needs to be applied to this proposed functionality.

This also suggests a decision point regarding the immediate future development of the ITA system. The current communication capabilities have been demonstrated and

exhibited proof of concept competencies. The communication capabilities can be further developed and expanded to provide a very important function to all of the involved entities. It is probably most desirable to invest near term money and time resources to bringing this functionally along to the desired level before investing resources in the applications within the analytical side. An even better recommendation is to focus on achieving the communication goals for the ITA system, while simultaneously achieving conceptual development work on the functional requirements of the analytical portion.

Bull's Eye Status Indicator

This is another component of the ITA system that is difficult to understand. Additional explanation in the user manual is needed. It is also unclear as to how each of the different status indicator attributes could be a different color. Can it mean the sender is not threatened by the event but the environment is? How does this relate to the societal attribute? Will the threat level (color) simply reflect the perception of the sender, or be established according to a specific evaluation protocol? Considerable attention needs to be assigned to establish the true functionality of this component.

Considering the human factors involved, there should be greater clarity in the color tint between the yellow and orange colors (or perhaps the monitors were at fault). The graphic status indicator should also include provisions for color-impaired workstation operators, or a requirement that all workstation operators have the full and complete ability to see, perceive, and understand all colors associated with the Homeland Security Advisory System.

During the demonstration, it was not clear why certain event status alerts were changed without complete knowledge of the incident. Since the Department of Homeland Security is the only entity that can change the alert status, it is necessary to consider connecting the ITA system to DHS, so that when the authorities change the alert status, the ITA system can facilitate direct communication of this change to all states and other participating entities.

Resources

As discussed in the above subsections, the availability of databases associated with any particular state will be very useful to the adjacent states whenever an incident occurs near their coexistent borders. These databases may be large and may take considerable amounts of time in order to be transferred to the inquiring ITA system workstation operator. This functionality needs to be more easily deployed without any impact to the system requirements and system resources currently being utilized. Also, as mentioned above, these databases need to be current and changes to them need to be accomplished in real-time, so everyone is knowledgeable regarding their availability. Information specialists found that merging data between adjoining states required considerable effort.

Event/Incident Cone Timeline

This feature was confusing, at best, to most observers and greater clarification of its function should be provided. This is assumed to be one of the analytical functions that has not yet been fully developed.

ITA USER RESOURCE DATABASES

One of the primary goals of the ITA system, as described to the evaluation team, is to include a significant number of databases, to which system operators would have access in real-time prior to or during an emergency. The demonstrated version of the ITA system contained a number of databases associated with the NMSHTD. They were:

- ❒ human resources;
- ❒ patrol yards;
- ❒ equipment locations;
- ❒ traffic control;
- ❒ fixed assets; and
- ❒ stockpile locations.

Using the Geographic Information System (GIS) capabilities imbedded in the current ITA system, an operator can define a geographical area and click on spatially located icons to gain access to a specific database of information. For example, by clicking on the Patrol Yards shape file and one of the spatially located icons, the resources available at that specific location are revealed. This includes job descriptions, job titles, names, and other important information. Thus, the ITA system provides an important organizing and access capability to system users. Ignoring emergency issues, this functionality is of prime value to all NMDOT managers and supervisors in the daily allocation of these resources to program needs. In addition, prior to an emerging emergency incident, or during an emergency incident, this capability may be of significant value in identifying available resources and matching those resources to operational demands. However, there are a number of issues that need to be understood and addressed before this capability is made available to all ITA workstations across all participating states. This subsection addresses these issues and suggests protocols.

Database Accuracy

The current version of the ITA system was demonstrated on July 3 primarily as a proof of concept exercise. However, the ITA system is fully functional in New Mexico and has been since April 2002. The databases represent real world information that may be accessed and used in the event of an emergency. Unfortunately those databases are currently static and represent a snapshot of the system's resources taken approximately 18 months ago.[12]

[12] The age of the databases was communicated by Mr. Tim Olivas, the LTAP Coordinator within the Research Bureau of the New Mexico State Highway and Transportation Department, during the late June visit to Albuquerque by the McCormick Taylor Evaluation Team.

The accuracy of the current information, particularly traffic engineering, and construction materials assets, for example, can be expected to be considerably distant from reality. This would be a major problem in the event of an emergency that would require decisions to be made and logistical applications to be implemented in real-time.

In order for the databases to be effective in real-time planning and response, it is necessary for their contents to be 100% accurate at every given moment. This means that a number of utilities would have to be developed and interfaced with the ITA system, so that accurate representation could be available. The following examples are offered to illustrate this requirement.

- ❒ The ITA system would need to be functionally tied to the entire roster of employees maintained by the NMDOT human resources department so that when changes to the roster occur, they would also be simultaneously posted in the appropriate ITA database. Such changes could be personnel additions, terminations, and short- and long-term disability situations, among others. In addition, the local patrol yard office would need to be able to update the database daily, with respect to what personnel are on vacation, taking a personal day, on jury duty, out sick, or otherwise on leave and consequently unavailable. This is needed so that true available human resources are identifiable for use in real-time resource allocation decision making.

- ❒ The ITA system would need to be functionally tied to a motor pool status-monitoring database that exhibits the availability and assignment of each item of equipment on a daily basis. Thus, only vehicles and equipment that are operationally functional would be listed. Those assigned to an individual or work crew and being used in the field would be so indicated along with their physical location. Conversely, any vehicle or item of equipment that is not functionally useful or currently being repaired would not be shown as available. For those vehicles and items of equipment being used in the field, it would be most desirable for each to be equipped with an automatic vehicle location (AVL) device, so that the ITA system can show (on a segment of the roadway network) its exact current location at the time of inquiry. Thus, the AVL system would need to be accessible by the ITA system. This is needed so that the true available vehicle and equipment resources are identifiable and locatable for use in real-time resource allocation decision making. In addition, each of these vehicles and equipment would need to be equipped with reliable radio or similar devices. In the event they or their operators need to be redeployed to an emergency activity location, the ITA operator or surrogate support personnel would be able to contact the appropriate persons and provide redeployment direction.

- ❒ During the interviews of stakeholders, it was identified that, even though equipment, personnel, and materials are available to be used in an emergency situation, consideration needs to be given to the planned use of those materials in the near future following the day(s) of the emergency event. For example, traffic control equipment may be planned for broad deployment on a construction project in the

days following an emergency event. That deployment may be part of a major logistical application of a large number and variety of government and private contractor resources. Preemptive use of these resources just prior to their planned use may cause serious schedule delays, consequently invoking penalties to the government as a result of non-performance clauses in signed contractual agreements.

- ❒ The same concept applies to each of the shape files identified above that are currently being used by the NMSHTD. Particular attention needs to be applied to any material inventories that might be queried and relied on, while looking for devices to use for emergency purposes. Likewise, this concern would apply to all states involved with the ITA system.

Additional Databases

The functional value of the NMSHTD database shape files to an ITA workstation operator associated with the NMSHTD is clearly important. Likewise similar databases would be of value to other segments within the emergency preparedness and emergency response communities, and in some cases, to all of the other governmental and private segments.

Transit Systems

The transit and paratransit systems in each state can and will play significant roles in all emergency preparedness and emergency response functions. It is consequently necessary to involve them in the emergency mobilization planning process, so that their capabilities can be effectively utilized when needed.

Transit and paratransit systems bring highly skilled managerial and administrative skills, associated with the operation and maintenance of vehicle fleets, that would be deployed in response to a need to evacuate large numbers of individuals from locations being flooded by extensive storms or attacked by a terrorism activity. In addition, bus vehicles have been proven to be useful as major barricades, when needed to support law enforcement activities. Paratransit vehicles are smaller by design and consequently have the ability to move into tight environments. This was proven in New York City after the events of September 11. In addition, these vehicles are equipped with lifts that would facilitate the needs of people with disabilities and those of age when an emergency occurs. It is clear that transit and paratransit resources are of major value to the ITA system.

Therefore, it is highly recommended that a database, indicating the spatial location of all transit facilities, be included in the ITA system. The database should include personnel attributes, in addition to vehicle and equipment attributes. Since many transit and paratransit systems are currently employing AVL equipment, ITA would need to be able to access the AVL system, so that the exact locations of resources could be established in real-time.

Fire Services

A shape file, illustrating the spatial location of each fire services unit along with the personnel and equipment resources, would be very useful in the event that a regional or statewide deployment of available resources is needed.[13] This would require each fire services facility to have individuals assigned to the timely maintenance of the personnel and equipment lists. Bar code images could be installed on each vehicle and read when each leaves the facility to reduce the need to input such data during an emergency response. This, of course, becomes problematic when the vehicles are taken outside their storage facilities for non-emergency activities (e.g., parades, washings). Automatic fire services personnel accountability is less easy to implement. However, information on the availability of fire services forces and their equipment would be of great value in organizing a response, whether to an act of terrorism or to a natural disaster such as a wildfire, hurricane, or flood.

National Guard

A shape file, illustrating the location of National Guard facilities, also seems necessary. It is understood that the governor of each state would make any decision regarding the involvement of the National Guard in emergency preparedness and emergency response activities. The spatial location of such facilities and a listing of the unclassified resources would help in real time when ITA system users are looking to mobilize all of the necessary resources. The Governor, or the National Guard units in each state, may be concerned that the availability of such databases may breach their security.

Hospitals and Other Medical Facilities

If the ITA system is used as part of a real-time emergency notification and response program, geographical displays of hospital and other medical facilities, along with some indication as to whether they are a trauma center and other specialty information, would definitely be valuable. At the least, the name of the emergency representative at each facility would be useful, so that they could be contacted as an event unfolds and needs are identified.

Medivac Helicopter, Ambulance and Emergency Medical Technician Resources

Similarly, geographic displays of Medivac helicopter, ambulance, and emergency medical technician resources would be useful in a deployment situation. In most states and

[13] The need for this information inventory to be accurate, as expressed in the above subsection, is very important. A real-time system would have to be interfaced with the ITA system, so that when vehicles and equipment are dispatched and consequently away from the staging location, they would be shown as unavailable. Similarly, if they have been assigned to mutual aid responsibilities when a nearby fire services unit has committed all of its available resources to an emergency, they would also be shown as unavailable. The goal would be for the ITA system to illustrate only those fire services resources that are available for assignment at the very moment of inquiry.

regions, 911 calls go to centers, where the nature and location of the event is logged and then redirected to the appropriate local response units. This is accomplished using a resource management software system. Developing a software utility that ties such software systems to the ITA system is believed to be more cost-effective than the development and maintenance of a separate database. Emergency medical deployment systems often address the problems of resource unavailability as a result of previous demands for service.

State and Local Law Enforcement Facilities

The geographical location of all state police barracks and other facilities, in addition to law enforcement facilities associated with municipalities and sheriff's offices, would also be valuable if included as a database in the ITA system. Although the station locations of law enforcement agencies are common knowledge information, the type and amount of vehicle and equipment fleets and personnel forces are critical information that should not be accessible to anyone other than authorized individuals. Law enforcement agencies may be reluctant to provide such database information, unless they are thoroughly convinced it will be securely available to only authorized users.

Heavy Equipment Providers

In the event of any kind of emergency, the availability of dump trucks, earthmovers, graders, cranes, and other heavy-duty specialty equipment becomes an important issue. A database in the ITA system, including the names of such companies, along with a general description of the types of equipment they own and are willing to lease, along with contact names and phone numbers, would be very valuable. Although, in an emergency, the cost of using such equipment may not be important, information in the database regarding rental costs may be useful in managing the efficient use of taxpayer monies.

Information on the ownership of the heavy equipment companies should also be considered, so that companies banned from public contracts as a result of poor past performances and companies identified as owned by organized crime members would be assigned a use as a last resort status. This latter issue is based on the experiences of the City of New York in the cleanup of the World Trade Center sites. It has been suggested that some of the vehicles and equipment were owned by, known or believed to be, organized crime members. Immediate response to significant incidents is important; however, post response follow-up by the news media, regarding questionable companies and individuals, needs to be avoided.

Others

The list established above is not meant to be comprehensive. Rather, it is designed to suggest that the concept of spatially locatable resources in ITA system resident databases would serve as a one-stop location for information necessary to make real-time decisions as an emergency is initiated, developed, and magnified. One must understand that this information needs to be maintained to reflect current availability, which may be difficult to

accomplish within the usually constrained budgets of many states. In addition, once such information is made available within ITA, the system becomes a significant treasure trove of important data to those individuals and groups intent on harming the US and its population. Thus, the absolute security of the included information becomes a very important requirement.

Restricted Access to Databases within ITA

The above paragraphs serve as a good segue to the issue of database accessibility. As the current ITA system is configured, it is potentially possible for each and every operator at an ITA workstation to have direct access to the databases within each state. This seems unnecessary. For example, the DOT in Maine will never need to know the locations of NMSHTD maintenance facilities and their associated personnel and resources. However, the Arizona DOT should have access to databases of the facilities within a certain distance of the physical border between New Mexico and Arizona.

Similarly, the availability of all of the mentioned and other databases to the Federal Government is very much unnecessary.[14] This information will be of significant value to the states in their preparation and response activities, but not to the Federal Government.

This suggests that an open architecture for the ITA system is unnecessary. Indeed, it further suggests that a central clearing house should be established, which controls the gateways to such databases by facilitating the application for access and approving necessary connectivity. This, in turn, suggests that the ITA system would require a central host, which controls all of the on and off switches associated with access by users to the various included databases (in whole or in part). The central host could be part of a government agency or a private contractor with the appropriate security clearances.

However the goal is attained, it is necessary to recognize that all ITA system workstations should not have access to all contained databases.

Timeliness of the Availability of Databases

The ITA system is conceptually very important for a large number of reasons, particularly as a result of the databases expected to be imbedded. Herein lies a new problem to be addressed. The data in the databases will only be useful to decision makers if it is available in real-time when needed. This means that the databases will need to be immediately available at the click of an icon. To achieve this goal, the databases cannot be expected to be transmitted via a phone line, at low transmission rates. Rather, the system requires high-speed, high capacity transmission capabilities. This requirement may negate the use of a standard VPN and may require a dedicated T1 communication cable to be installed to connect each ITA workstation.

[14] It was commonly expressed by those Federal Government employees interviewed during the July 3, 2002 demonstration that the Federal Government has not and would not have any need for this information prior to, during, or after an incident of merit.

The accuracy of the available databases, in critical response deployments, was addressed above. Equally important is the need to have this accurate data available immediately upon request. This is related to the above issue concerning the limited availability of all databases to all ITA system workstations. If all databases are available, and access to them is occurring simultaneously for large numbers of users, the overall ITA system would require very high capacity throughput capabilities. Current technology may not be sufficient to handle such data volumes. In other cases the portal attributes on file sizes may need to be expanded considerably beyond typical communication requirements.

This causes consideration of another potential problem, that of virus detection and handling software systems and security software systems. Some such systems look for situations whereby large files are being downloaded into the ITA system workstation, or being uploaded from the ITA system. When detected, they automatically truncate the flow of information, assuming that someone is stealing large files and/or that someone is infecting the workstation with a large file. In either case, this will need to be considered during the development phase of the functional requirements for the ITA system.

ITA TRAINING AND OUTREACH

This subsection of this appendix advises NCHRP on the training and outreach aspects concerning the ITA system.

Training

ITA system training will require a major effort on the part of the entity responsible for the full deployment of the ITA system across the country and the transportation agencies requiring training. Specific guidelines designed to aid with ITA documentation and training are provided below.

Extensive Documentation

The ITA system is currently in a developmental phase. Each step taken to improve the system must be documented and stored in an organized fashion. This information can then be used to develop and administer the necessary training programs. It can also be used to market and sell the ITA system to potential end users. Any changes made to the ITA system should be dated, saved, backed up, or duplicated, and stored in a secure environment. Plans for the creation and betterment of the ITA system should also be placed in trusted hands. Should the nation decide that the ITA system is to be the dominant communication system (and eventually the analytical system); all information concerning ITA must be absolutely secure.

Detailed Training

Extensive detailed training of ITA system workstation operators is required for the system to be successful. During the July 3 demonstration, there was an element of significant confusion among the observers and operators who did not quite understand each of the

six quadrants of the base display and their value within the system. Operators with insufficient training on the use of the system's functionalities will be a problem during any emergency.

The ITA system oversight entity should deploy a team of trainers to each site where an ITA workstation will be installed. The team should be constructed from individuals with various backgrounds: information systems technology and operational experience in the application of the ITA system to disaster and other emergency incidents. Training sessions should be hands-on and supported with many handouts and diagrams to ensure that all system functionality and use is conveyed to the workstation operators. Checklists (such as the one used previously in the ITA Call Center and Notification subsection of this appendix) should also be developed and used to outline protocols associated with the system.

Outreach

ITA system outreach is intended to encourage state DOTs and other transportation, security and law enforcement agencies to become users of this breakthrough in security communication and analysis technology. Some suggestions for the future marketing and implementing of the ITA system are described below.

Capabilities of the ITA Software System

Many agencies present at the July 3 demonstration expressed that they would have preferred to be provided with much more information on the ITA system prior to the demonstration. Because they did not fully understand the screens and the functionality of the system, their impressions were colored by the technical difficulties that were periodically experienced. A basic amount of exposure training prior to the demonstration may have helped these transportation professionals to recognize the current capabilities of the ITA system. Some said they thought, going into the demonstration, that ITA had more communication and analysis capabilities than it actually does at this time. This caused some of them to believe that the system was a bit oversold.

This is disappointing since the ITA system really sells itself when it is reliably and consistently functioning. Many transportation and security professionals were impressed with the ideas presented and were able to talk freely concerning the capabilities of the ITA system. They were mostly delighted that the ITA system was able to spark discussion on the need for a sophisticated and secure communication and analysis system. They seemed to understand that the system needs further development, but expected somewhat more information regarding the alert status level indicator, event cone, and operational plans. These specific quadrants require considerable further development as was discussed in the subsection Communication and Analytical Functionality; however, they really are part of the analytical side that is still primarily in the conceptual stages. As an aside, the operational plan functionality is book-marked to allow local users to post their emergency response scenarios, so that, in the event of an emergency, they will be able to immediately access their situational plans. This assumes that electrical power is available. This suggests that

the ITA system requirements need to include an uninterrupted power supply and an emergency power generation system. This could add substantially to the basic startup cost estimate of $5,000 per workstation. However, if multiple ITA system workstations were deployed in the same facility, only one power generator would be needed.

Coordination with Various Agencies

It was evident from the demonstration that each transportation agency currently has a different way of communicating safety and security threats to other personnel within the agency, among transportation and law enforcement agencies, and up the ranks to the US DOT and other government officials. Many different relationships with personnel at these various levels have been created. For instance, MDOT has created long-term relationships with all members of the I-95 Corridor Coalition, populated with transportation agencies from Maine to Virginia. These relationships are now nearly five years old and have matured substantially. MDOT prides itself on the bonds that enable its personnel to freely contact each transportation agencies belonging to the I-95 Coalition and discuss interstate transportation concerns.

In contrast, the Maryland State Police have a different way of conducting communications. The sergeant assigned to MDOT serves as a liaison to the Maryland State Police, in the event that a major transportation incident occurs and law enforcement services are needed. Otherwise, the dissemination of general threat information is desired to be handled in a top to bottom fashion. When a new communication and/or information system is introduced to the state DOT or other transportation agency, everyone is encouraged to discuss the system and talk openly. When a new system is introduced to the state police, it is generally established at the highest-ranking levels first, and disseminated slowly down the ranks on a need-to-know basis over time. Members of the Team were told that it is considered disrespectful if a lower-ranking officer brings information on communication and information systems to the desk of the higher-ranking officer.

In future activities involving the ITA system at the state level, law enforcement entities should be approached initially at the highest level, so that decisions can be made and the flow of information (and assigned participation) can be funneled down the command chain.

The challenge of introducing a new, sophisticated software system to each agency is being able to recognize how each operates and communicates before impressing the system upon the department that will be responsible for it. ITA system proponents must understand the general inner-workings of each agency's communication infrastructure before they actually suggest installation at the site. It is suggested that ITA system proponents ask many questions of each user agency, such as, "Am I speaking with the right person concerning this matter?" The provided response must be carefully listened to and understood. This is critical to establishing a working relationship that will mature and foster inclusion of the ITA system at the agency. It is important for ITA system personnel to be considerate of the systems already in place at transportation and other agencies. This will perhaps increase the chances that local professionals will be eager to consider purchasing the new ITA software system.

ITA COSTS

Although not part of the evaluation of the ITA system demonstration, the cost of implementing the existing ITA system or enhancing the existing system and implementing the new version is a relevant issue. The McCormick Taylor Research Team's Principal Investigator, Mr. John N. Balog, had a telephone conversation with NMSHTD's Mr. David Albright on July 10, 2002 that included the topic of cost. This information is reported here in order to maximize the comprehensiveness of this evaluation.

Several cost elements are appropriate to mention:

- ❒ the initial startup cost of an ITA workstation in each state department of transportation office and at the offices of other relevant entities;
- ❒ the cost associated with further development and enhancement of the communications component of the ITA system; and
- ❒ the cost associated with the development of the analytical capability component of the ITA system.

Each is addressed below.

Initial Startup Costs

Mr. Albright indicated that the initial cost of purchasing the hardware and software necessary to establish an ITA workstation along with its installation is approximately $5,000.00 and should be borne by each of the states and other entities interested in local deployment. Functional specifications should be developed for the hardware and software so that all ITA workstations will have the same capabilities. Purchase of all of the equipment via a state contract using the same vendor would contribute to the uniformity necessary to maximize reliability and consistency.

The cost of staffing the workstation and related items such as office space, printers, and flat wall size monitors, etc. should be borne by the states.

Enhancement of Communications Component Costs

Mr. Albright indicated that the remaining monies associated with this task order could be applied to contributing to the development of the functional requirements for the communications component. He indicated that an additional $1.5 million of federal funding should be made available to enhance the communications component over approximately a period of one year. National laboratories, state DOTs and private industry may individually or in combination be responsible for accomplishing this work.

Once the initial development is completed, any necessary enhancement work would need to be funded on an annual basis by the federal government.

Mr. Albright indicated that ongoing maintenance and technical support for the ITA system would be expected to be provided by the private sector under contract to the US Department of Transportation.

Development of the Analytical Component Cost

The analytical component of the ITA system is currently less developed than the communications component. Mr. Albright believes that the development of this component will take approximately 5 years and cost approximately $15 million. National Laboratories, private industry, or a combination of the two can best accomplish the work. Since the analytical portion is intended to help forecast terrorism events with potential consequences to the nation, Mr. Albright believes that the federal government should provide the funding for this effort.

It needs to be stressed that these estimates are based on the information that is available today and may vary as additional work is accomplished and the challenges become better understood or evolve.

OTHER ITA FINDINGS

A full discussion of the ITA system must include four aspects of the software believed to be the least evolved and consequently most difficult for the average user or observer to understand. These aspects are the alert status indicator, the event cone, the prospect for data mining, and the operational plans.[15] These aspects of the system, once developed, are expected to dramatically augment the capabilities of the ITA system. However, everyone involved in the program would certainly admit they are not currently available to users and some may be many years away from their ultimate potential application.

Alert Status Level Indicator

Perhaps nothing within the ITA system, with the possible exception of the map of the United States in the GIS user interface partition, attracts as much attention as the alert status level indicator. Its ability to illustrate the various concerns (user, vehicle, infrastructure, social, and environmental), using the colors of the Department of Homeland Security, adds to this attraction. Unfortunately, the reasons for the indicator's target-like appearance are less understood. As was presented to the team, the possibility exists to highlight a specific type of threat by sending a message, for instance, about an accident with a tanker truck carrying hazardous materials that resulted in a spill. As was explained, such a circumstance might highlight the threat rings concerning the vehicle and environment as red. If the hazardous material was flammable or corrosive, there could be a threat to infrastructure as well,

[15] Some of these topics have also been addressed in either a detailed or brief fashion in earlier subsections of this appendix. This was done because they fit nicely into the then current topic of a previous subsection. They are further addressed here as a standalone subsection because of their importance to the future development of the ITA system.

which would also be displayed as red. If evacuations were warranted, there might presumably be a societal threat, also distinguished by red. If the caller (user) passed by the accident site as it happened and called in the accident as he/she continued to drive away and is not or will not be directly affected, the user ring may be illuminated as green.

It is difficult to say how this aspect of the system will eventually come to be used. For the present time, however, this ability to differentiate threat levels by affected element is confusing, since there are no identifiable protocols established for assigning the threat levels (colors). The establishment of such protocols, with very rigid definitions, needs to be accomplished if this aspect of the ITA system is to become functionally acceptable. It is believed that extensive analysis will be needed in order to be able to define and classify all of the threats and the interrelated impact they may/will have on the five elements. The developed protocols have to be very easy to understand and to apply, since the call center operator will need to make instant decisions as to the assigned color levels in real-time. Likewise, all ITA system workstation operators will need to be trained, so that they fully understand the meaning of the applied colors in every threat instance. An item such as this, that draws one's instant attention, must be more effectively defined as soon as possible. It also needs to be clearly defined that the colors have been assigned by the user and despite the fact they are the same as those used by the DHS, DHS has not assigned the alert level represented by the color.

Setting and Changing Alert Levels

As conveyed by some participants and many observers of the July 3 demonstration, there may be some fundamental problems with the alert levels, as portrayed in the demonstration scenario. It is understood that the scenario was simply a way to demonstrate the software's capabilities. Yet, this use may also reflect certain underlying thinking as to how alert levels might be set or changed in the event of an actual incident.

It was troubling to many of the observers that the states or others changed the alert levels in the demonstration. The DHS (not the FBI or the US DOT), as the audience for the demonstration was very aware, is singularly responsible for setting the alert levels. This also gives rise to the issue of transmitting a threat level via an ITA system message. There was a minor complaint that this was cumbersome, particularly since each of the elements had to be treated individually using a dropdown box. It was suggested that the levels could have been more easily applied if it were possible to start from the alert level of the last outgoing message. This would save keystrokes. However, it might contribute to the workstation operator not taking the time to appropriately digest the known information and to apply the color scheme in an accurate manner. Other users found it troubling that they were required to establish their own alert levels as they composed and sent a message. Many also found it difficult to understand how coloring the elements could be message-dependent. The concept becomes more complex when a series of messages are associated with a single primary incident. Do the color labels remain constant[16] for each of these messages? Or

[16] If so, can the ITA system software cause this to happen without the need for the workstation operator to make decisions?

can each new message have a different combination of colors, as defined by the message sender? If this is the case, it becomes very confusing to others who are monitoring the messages to understand the true, actual alert level. Additional thinking is required to bring the functionality of this part of the basic system to a level that is useful.

Silent Alert Levels

When the DHS establishes the alert level, it is immediately broadcast to everyone so that, if necessary, heightened actions can be initiated. This includes the news media. During the demonstration, it was mentioned that the ITA system could convey a silent alert level to the participating states and other entities. The news media would not be aware of the change and administrators would have the time to make the necessary decisions before having to deal with the media. However, any entity not member to the VPN would not be aware of the change in status at the same time as the states. This is despite the fact that the municipalities and states may be dependent on each other when applying resources to the resolution of the threat. The concept of a silent alarm seems to be oxymoronic, particularly since the alert levels devised by the DHS were devised as an easily understood way of communicating to the general public the overall degree of danger present at any given time.

Event Cone

The event cone within the program represents an interesting concept that, if developed to the fullest extent, will be of considerable value to the states and the country. However, at the present, it is inoperative. This caused many observers and participants to question its function and how it will operate. As discussed in one of the earlier subsections of this appendix, the event cone is intended to graphically depict the status of an unfolding event and to predict when something can be expected to occur. In theory, the events associated with a threat are indicated left to right as time progresses and come to a head, with a common point at the location, at which an event is forecasted to occur. The lines representing each segment then begin to diverge, as the situation is gradually resolved.

Discussions between the Principal Investigator and Mr. David Albright have determined that this is part of the analytical portion of the ITA system that will require considerable research and development before becoming fully functional. This can be interpreted to mean the solution is not currently determined and may take a considerable amount of time before it becomes a reality.

Data Mining

Like the event cone, the prospect of future data mining is intriguing but not yet functional. The ITA system will be collecting significant amounts of data on a daily basis. Some of that data will instantly reveal information that must be acted upon immediately. Data mining is less direct. It refers to the concept of being able to string together certain apparently dissimilar and unconnected items of information, usually from one, or a series, of databases into a comprehensible whole. For example, the ITA system may be provided information that the metal fencing outlining the perimeter of a dam was cut to generate an

opening large enough for a human to enter. No evidence was found other than the hole in the fence and no attack occurred. Similar incidents involving other dams over time would suggest that dams are a target for a conspiratorial activity. Data mining should be able to recognize the similarity of the individual events and combine them into a hypothesis that will be needed to be tested for validity. Ultimately, the conclusion may be that a coordinated attack on dams should be expected, so that mitigation and prevention measures can be installed. The ITA system demonstrated on July 3 does not yet have this capability. This is understandable, since the real test was to demonstrate the four competencies in a proof of concept exercise and data mining was not targeted for competency. However, it was found that many observers in the demonstration had come to previously believe that the ITA system currently had this capability. Until this capability has been fully developed and demonstrated to competency, its mention in discussions should simply indicate that it is the intent for the system to be able to achieve data mining in the future and that research is on-going as to how this can be accomplished.

This capability, when developed, will require considerable human intervention in developing key words and phrases to be searched for in the databases. The automation side will be to identify events with the key words or phrases and to present them to a human for processing. This may require a considerable number of analysts. Their spatial work location and the organization they will be working for is yet to be determined. Ultimately, as the concepts and applications of artificial intelligence are further developed and made useful to this kind of activity, the need for human intervention will be reduced. It is currently unknown when this may occur in the future. In addition, artificial intelligence applied to the Call Center would be valuable if it could automatically ascertain the seriousness of incoming calls and route them appropriately to the safety, security, or other call list category for response.

Data mining will need to be applied to older historical time-series data to establish longer-term trends. It will also need to be applied to cross-section data for the same date so that conspiratorial actions can be identified. Functional requirements for both of these capabilities need to be defined.

Emergency Operating Plans

The ITA system component dealing with emergency operating plans is not yet fully active. NMSHTD has developed a number of emergency scenarios for which emergency operational plans have been created. It is unknown as to whether they are currently resident within the ITA system. The concept is to identify as many potential threat realization activities as possible and to develop emergency response plans. In contrast to a Standard Operating Plan (SOP), which defines the normal day-to-day steps in the process, an Emergency Operating Plan (EOP) defines the steps to be implemented when an emergency event occurs. Such plans are designed to be able to be implemented immediately and without real-time forethought. By training and drilling appropriate personnel, in the aspects of the EOPs, the state or participating entity is prepared to instantly act when an identifiable event occurs. Storing these plans on the ITA system guarantees immediate access and dissemination as needed. This is an excellent idea.

It would be useful to conceptually define the development of EOPs and how to include them in the ITA system so that adopting states can initiate their development and inclusion. It is believed that many states probably already have extensive EOPs in place. In such cases, it would be valuable for them to add the EOPs to the ITA system. Since this is simply a Word document recall effort, it should be easy to accomplish. However, additional research should be accomplished to determine whether some of the information and processes in each EOP should be automated to the extent that, once the plan is accessed, notification to all key managers and other decision makers is readily made, causing the deployment of personnel and equipment as necessary to respond to the event.

The concept of including EOPs in the ITA system was tantalizing to some observers in an Emergency Operations Center (EOC) environment. If an expanded application of the system were, for instance, able to utilize artificial intelligence to identify various components of set plans to create a wholly new plan in response to an event which was previously not identified and planned for, the ability to effectively respond to most events would be greatly enhanced. The research and development associated with this aspect of the ITA system is expected to require significant resources both in personnel and time.

The less dynamic portion of this application might well offer the most near-term promise. EOC personnel could immediately access the EOP without being dependent on human memory. The technology would assist them. Many EOC duty rotations involve 12-hour shifts for the duration of an emergency action. There is an obvious tendency for people in these positions, however professional, to become tired and forgetful. The beauty of the computer is that, if the program is working properly, it has no such limitations and could prompt or remind a human actor that certain actions were needed, even monitoring whether certain phone calls were made or other actions were taken. Such applications might ultimately need to be highly customized, depending upon individual emergency plans. As stated elsewhere in this document, there is also a need, in an EOC environment, for the system to be straightforward, easy to use, and well documented. EOCs tend not to be involved with emergency operations for large periods of time, just prepared for activation. When the center is mobilized, there needs to be a minimal learning curve on remembering how to use systems that may have sat idle for some time.

EXHIBIT A-1: PRE-DEMONSTRATION STRUCTURED TOPIC GUIDE CONTENT

SECURE COMMUNICATION INFRASTRUCTURE
STRUCTURED TOPIC GUIDE
PRE-ITA DEMONSTRATION VERSION

Date of Interview: _____
Interviewer's Name: _____
Location of Interview:_____

Write all collected information and any other responses in this topic guide.

TO INTERVIEWER: **Please convey the following message to each of the individuals you are interviewing at the start of each session. It is best to memorize the materials as opposed to reading this introduction.**

TO INTERVIEWEE: Thank you for meeting with me. I would like to explain to you my role in the ITA scenario exercise that will be occurring this coming Wednesday. I am with McCormick Taylor, Inc. a Philadelphia-based consulting firm that has been engaged by the National Academy of Sciences, Transportation Research Board to provide an impartial, objective evaluation of the ITA system. One of the roles of McCormick Taylor will be to assist in any future augmentation or changes to the system so that its maximum value can be realized. I will be raising some topics and I would appreciate your responding as you see fit. Feel free to elaborate to whatever degree you desire. Also if you do not understand the issue or need further clarification, just ask me to elaborate.

Do you have any questions before we start?

TO INTERVIEWER: PLEASE EXCHANGE BUSINESS CARDS SO THAT YOU CAN EFFICIENTLY GET THE FOLLOWING DEMOGRAPHIC INFORMATION. If they do not have a card, ask for the information.

Name of Interviewee: _____
Title: _____
Organization: _____
Address: _____
Phone: _____
Fax: _____
E-mail Address: _____

1. **Please tell me about your involvement with ITA to date?**

2. **How do you anticipate the ITA system will assist you in performing your job?**

3. **What specific applications do you expect to see for the ITA system in your region?**

4. **What specific applications do you expect to see for the ITA system in the rest of the country?**

5. **Tell me about the level of information you have generally had regarding emergency and other safety and security events in other states?**

6. **The ITA system is designed to provide you with information regarding emergency and other safety and security events in other states. How will knowing about such emergency and other safety and security events in other states help you to fulfill your job at your agency?**

7. **What do you think you will learn from the July 3rd demonstration?**

8. **How do you see ITA changing your relationship with other preparation and response professionals in your region?**

9. **The ITA call center serves as the access to the entire system. What do you expect to be its most significant features?**

10. **Do you have any ideas regarding how the call center capabilities can be enhanced?**

11. **Please describe your level of comfort regarding the sharing of emergency and safety and security information with other states.**

12. **How important is it to you to receive any and all threat information prior to hearing about it from the news media? Please expand.**

13. **How effective are the news media in helping you prepare for and respond to threats?**

14. How do you feel about using the ITA system via the Internet, to access threat and response information?

15. How important is it to you to be able to access the ITA system via the Internet or via an ITA workstation?

16. What is your experience with software systems that display detailed maps of your state and its transportation network?

17. What do you think of the ITA system's ability to display detailed maps of your state and its transportation network during an emergency event?

18. How important is it to you in your job to be able to access many different databases of resources via the ITA system (i.e. human resources, patrol yards, equipment locations, traffic control, fixed assets, stockpile locations, and other resources)?

19. What issues or capabilities are important to you regarding the ITA system that we have not talked about during this interview? Please expand your thoughts.

TO INTERVIEWEE: I will be interviewing you after the ITA demonstration to get your impressions of the exercise.

I would appreciate your continuing cooperation at that point.

Thank you for assisting us in the evaluation of the ITA system.

If you need to speak with me in the mean time feel free to call me at PHONE NUMBER.

Thank you again.

EXHIBIT A-2: POST-DEMONSTRATION STRUCTURED TOPIC GUIDE CONTENT

MTA SECURE COMMUNICATION INFRASTRUCTURE
STRUCTURED TOPIC GUIDE
POST ITA DEMONSTRATION VERSION

Date of Interview: _____ Time of Interview: _____AM/PM
Interviewer's Name: _____

Write all collected information and any other responses in this topic guide.

TO INTERVIEWER: Please convey the following message to each of the individuals you are interviewing at the start of each session. It is best to memorize the materials as opposed to reading the introduction.

TO INTERVIEWEE: Thank you for allowing me to debrief you regarding the ITA demonstration on July 3. Again, I will remind you of my role concerning the ITA scenario exercise. I am with McCormick, Taylor & Associates, a Philadelphia-based consulting firm that has been engaged by the National Academy of Sciences, Transportation Research Board to provide an impartial, objective evaluation of the ITA system. One of the roles of McCormick Taylor will be to assist in any future augmentation or changes to the system so that its maximum value can be realized. I will be raising some issues and I would appreciate your responding as you see fit. Feel free to elaborate to whatever degree you desire. Also if you do not understand the issue or need further clarification, just ask me to elaborate.

Do you have any questions before we start?

TO INTERVIEWER: If you did not receive a card or demographic information in the pre-ITA interview, request the following information. Also, please make sure that the interviewee's information did not change since the pre-ITA interview.

Name of Interviewee: _____
Title: _____
Organization: _____
Address: _____
Phone: _____
Fax: _____
E-mail Address: _____

1. Please provide your overall impressions regarding the ITA demonstration on July 3, 2002.

2. What characteristics of the ITA software system impressed you the most? Please explain.

3. What characteristics of the ITA software system require the most improvement? Please explain.

4. Please describe your thoughts as to how the ITA software system can be best used at your agency in the foreseeable future.

APPENDIX B: DEVELOPERS AND END-USERS INTERVIEWED FOR FEATURES MATRIX

Table B-1 identifies the 23 professionals contacted/interviewed during the conduct of this Task Order. Included is the name of each software system, their role as a developer of the software or a user of the software, his or her contact information, the professional who conducted the interview, and the date the interview was completed.

TABLE B-1: INTERVIEWED DEVELOPERS AND END-USERS

SYSTEM NAME	INTERVIEWEE	DEVELOPER OR END-USER?	INTERVIEWER	INTERVIEW DATE
AIM	John Bowles E Team Project Manager 7301 Topanga Canyon Blvd. Suite 300 Canoga Park, CA 91303 530-672-2468 f. 775-255-4109 <jbowles@eteam.com>	Developer	Andrew Lofton	05/20/03
AIM	Lt. Paul Faucett US Coast Guard US DOT Crisis Management Center (CMC) DOT NASSIS BUILDING CMC Room 8332 400 7th Street, NW Washington, DC 20590 202-366-1863 f. 202-366-3768 <pfaucett@comdt.uscg.mil>	End-User, Transportation Industry	Andrew Lofton	05/17/03

TABLE B-1: INTERVIEWED DEVELOPERS AND END-USERS

SYSTEM NAME	INTERVIEWEE	DEVELOPER OR END-USER?	INTERVIEWER	INTERVIEW DATE
DMIS	Richard Munnikhuysen Program Manager Battelle 24 Center Street Stafford, VA 22556 540-288-5623 f. 540-288-5601 <munikhr@battelle.org>	Developer	Peter N. Bromley	06/06/03
DMIS	Charles Bell Chief, Defense Consequence Management Systems Office PM NBC, Marine Corps Systems Command 2033 Barnett Avenue, Suite 513 Quantico, VA 22134 703-432-3212 f. 703-432-3204 <bellc@mcsc.usmc.mil>	End-User	Peter N. Bromley	06/06/03
InfraGard	Mitzi Madere Content Manager Louisiana State University 402 Johnston Hall Baton Rouge, LA 70803 225-578-9252 f. 225-578-9235 <mitzi.l.madere@infragard.org>	Developer, System Administrator	Jamie Beth Strongin	05/28/03

TABLE B-1: INTERVIEWED DEVELOPERS AND END-USERS

SYSTEM NAME	INTERVIEWEE	DEVELOPER OR END-USER?	INTERVIEWER	INTERVIEW DATE
InfraGard	Michael Litchfield Content Coordinator Louisiana State University 402 Johnston Hall Baton Rouge, LA 70803 225-578-0899 f. 225-578-9235 <michael.litchfield@infragard.org>	Developer, System Administrator	Jamie Beth Strongin	05/28/03
InfraGard	A. Brett Hovington Supervisory Special Agent Federal Bureau of Investigation 935 Pennsylvania Avenue, NW Washington, DC 20535 202-324-3000 <bhovington@fbi.gov>	Developer and End-User, Program Manager	Jamie Beth Strongin	05/29/03
InfraGard	Jane B. Marazzo Special Agent Philadelphia FBI 600 Arch Street, 8th Floor Philadelphia, PA 19106 215-418-4000 <infragard-ph@fbi.gov>	End-User, Chapter Coordinator	Jamie Beth Strongin and John N. Balog	06/02/03

TABLE B-1: INTERVIEWED DEVELOPERS AND END-USERS

SYSTEM NAME	INTERVIEWEE	DEVELOPER OR END-USER?	INTERVIEWER	INTERVIEW DATE
InfraGard	John Chesson Special Agent Philadelphia FBI 600 Arch Street, 8th Floor Philadelphia, PA 19106 215-418-4000 <jchesson@fbi.gov>	End-User, Chapter Coordinator	Jamie Beth Strongin and John N. Balog	06/02/03
InfraGard	Phyllis A. Schneck, Ph.D. VP Enterprise Services eCommSecurity 30 Perimeter Park Drive Suite 200 Atlanta, GA 30341 770-216-9990, ext. 3016 f. 770-216-9330 <pschneck@mindspring.com> or <phyllis.schneck@ecommsecurity.com>	End-User, Chair of InfraGard's National Executive Board	Jamie Beth Strongin	On 05/29/03 Dr. Schneck was requested to coordinate with private industry users to complete responses to the matrix question-naire and to return them as soon as possible. The responses were not received in time to be included in this document.

TABLE B-1: INTERVIEWED DEVELOPERS AND END-USERS

SYSTEM NAME	INTERVIEWEE	DEVELOPER OR END-USER?	INTERVIEWER	INTERVIEW DATE
ITA (CURRENTLY DEPLOYED PROTOTYPE)	Timothy J. Olivas Local Transportation Assistance Director (LTAP) New Mexico State Highway and Transportation Department 7500 Pan American NE Albuquerque, NM 87109 505 841 9152 f. 505 841 9163 <timothy.olivas@nmshtd.state.nm.us>	Developer	John N. Balog	07/18/03
ITA (CURRENTLY DEPLOYED PROTOTYPE)	Terry Simmonds Emergency Management Program Manager Washington State DOT PO Box 47358 Olympia, WA 98504-7358 360-705-7857 f. 360-705-6823 <simmont@wsdot.wa.gov>	End-User, transportation	Peter N. Bromley	06/10/03

TABLE B-1: INTERVIEWED DEVELOPERS AND END-USERS

SYSTEM NAME	INTERVIEWEE	DEVELOPER OR END-USER?	INTERVIEWER	INTERVIEW DATE
ITA (CURRENTLY DEPLOYED PROTOTYPE)	Rick Horton Information Technology (IT) Support Washington State DOT PO Box 47358 Olympia, WA 98504-7358 360-705-7856 f. 360-705-6823 <rlhorton@wsdot.wa.gov>	End-User, transportation	Peter N. Bromley	06/10/03
ITA (PROPOSED NATIONAL SYSTEM)	Michael Moulton Project Manager Sandia National Laboratories Department 5845 Mail Stop 0759 Albuquerque, NM 87185-0759 505-845-8106 <mwmoult@sandia.gov>	Developer	John N. Balog	07/18/03
IRRIS	Alan K. Beiagi Director of Advanced Technologies GeoDecisions 207 Senate Avenue Camp Hill, PA 17011 717-763-7211 f. 717-763-8150 <abeiagi@geodecisions.com>	Developer	Jamie Beth Strongin	05/30/03

TABLE B-1: INTERVIEWED DEVELOPERS AND END-USERS

SYSTEM NAME	INTERVIEWEE	DEVELOPER OR END-USER?	INTERVIEWER	INTERVIEW DATE
IRRIS	Paul W. Allred Chief, Highway Engineering Team Military Traffic Management Command Transportation Engineering Agency (MTMCTEA) 720 Thimble Shoals Blvd. Suite 130 Newport News, VA 23606-4537 757-599-1170 f. 757-599-1682 <paul.allred@tea.army.mil>	End-User	Jamie Beth Strongin	06/05/03
IRRIS	Douglas Plummer Watch Analyst US DOT CMC DOT NASSIS BUILDING CMC Room 8332 400 7th Street, NW Washington, DC 20590 202-366-5740 f. 202-366-3768 <douglas.plummer@rspa.dot.gov>	End-User, Transportation Industry	Peter N. Bromley	06/16/03

TABLE B-1: INTERVIEWED DEVELOPERS AND END-USERS

SYSTEM NAME	INTERVIEWEE	DEVELOPER OR END-USER?	INTERVIEWER	INTERVIEW DATE
MobileShield™	Royce Kincaid Wireless Program Manager Northrop Grumman 4805 Stonecroft Blvd. Chantilly, VA 20151 703-633-8300, ext. 4146 f. 703-449-9352 <rkincaid@northropgrumman.com>	Developer	Andrew Lofton	05/23/03
MobileShield™	Phil Buvia Homeland Security Division Northrop Grumman TASC 4805 Stonecroft Blvd. Chantilly, VA 20151 703-633-8300 <pbuvia@northropgrumman.com>	End-User	Andrew Lofton	05/28/03
ST-ISAC	Paul G. Wolfe Vice President and ISAC Director EWA Information & Infrastructure Technologies, Inc. 13873 Park Center Road Suite 200 Herndon, VA 20171 703-478-7656 f. 703-478-7654 <pwolfe@ewa.com>	Developer, Operator	Peter N. Bromley	05/21/03

TABLE B-1: INTERVIEWED DEVELOPERS AND END-USERS

SYSTEM NAME	INTERVIEWEE	DEVELOPER OR END-USER?	INTERVIEWER	INTERVIEW DATE
ST-ISAC	Steven P. Clemmons Technical Director EWA Information & Infrastructure Technologies, Inc. 13873 Park Center Road Suite 200 Herndon, VA 20171 703-478-7657 f. 703-478-7654 <sclemmons@ewa.com>	Developer, Operator	Peter N. Bromley	05/21/03
ST-ISAC	Greg Hull Director of Operations Safety and Security Programs American Public Transportation Association (APTA) 1666 K Street, NW Washington, DC 20006 202-496-4815 f. 202-496-4331 <ghull@apta.com>	End-User	Peter N. Bromley	05/22/03
ST-ISAC	Director of Security US Railroads Name and contact information withheld per request	End-User, Transportation Industry	Peter N. Bromley	05/30/03

APPENDIX C

PRINCIPAL SECURITY CONTACTS AT STATE DOTS - JANUARY 2004 (updated 01/05/04)

STATE	*NAME*	*PHONE*	*FAX*	*E-MAIL*
Alabama	John Lorentson, Maintenance Engineer	334-242-6272	334-242-6378	lorentsonj@dot.state.al.us
Alaska	Frank Richards, State Maintenance and Operations Engineer	907-465-3906	907-586-8365	frank_richards@dot.state.ak.us
Arizona	Lonnie Hendrix, ADOT Central Maintenance	602-712-7972	602-712-6745	lhendrix@dot.state.az.us
Arkansas	Ralph Hall, Assistant Chief Engineer - Operations	501-569-2221	501-569-2221	Ralph.Hall@ahtd.state.ar.us
California	Patricia Kuhar, CISSP, IAM Chief Information Security Officer	916-651-8483	916-799-5907	patricia_kuhar@dot.ca.gov
Colorado	Elbert Hunt	303-273-1849		elbert.hunt@dot.state.co.us
Connecticut	Dave Crowther, Director of Management Services	860-594-3032	860-594-3008	Dave.Crowther@po.state.ct.us
Delaware	Patricia Faust, Planner, ITS Division	302-659-2407	302-659-6128	pfaust@mail.dot.state.de.us
D.C.	Natalie Jones, Emergency Preparedness Manager	202-671-0539	202-671-0650	natalie.jones@dc.gov
Florida	Frank Day, Emergency Coordination Officer	850-245-1505	850-245-1552	frank.day@dot.state.fl.us
Georgia	Georgene Geary, State Materials and Research Engineer	404-363-7512	404-362-4925	georgene.geary@dot.state.ga.us
Georgia (2)	Stephen Henry	404-656-5214	404-463-7071	stephen.henry@dot.state.ga.us
Hawaii (1)	Kelvin Ogata	808-587-2623	808-587-6306	kelvin.agata@hawaii.gov
Hawaii (2)	Glenn Yasui sent 12/10	808-587-2220		Glenn.Yasui@hawaii.gov
Idaho	Bryan Smith, Emergency Management Coordinator	208-334-8414	208-334-8595	bdsmith@itd.state.id.us
Illinois	Joe Hill, Chief of Operations	217-782-7231	217/782-1927	Hilljs@nt.dot.state.il.us
Illinois (2)	David Phelps, Assistant Secretary of Transportation	618-549-0699	618-351-6268	Phelpsdd@nt.dot.state.il.us
Indiana	Rick Smutzer, Chief Engineer	317-232-5529	317-232-0238	rsmutzer@indot.state.in.us
Iowa	Raymond Callahan, Emergency Management Coordinator	515-239-1678	515-239-1005	raymond.callahan@dot.state.ia.us
Kansas	Susan Barker, Staff Engineer, Construction and Maintenance	785-296-3576	785-296-6944	susanb@ksdot.org
Kentucky	Gary Mitchell	502-564-4556	502-564-2978	gary.mitchell@mail.state.ky.us
Louisiana	Gordon Nelson, DOTD Assistant Secretary, Operations	225-379-1210	225-379-1861	gnelson@dotd.state.la.us
Louisiana (2)	Joe Modicut, Chief of Emergency Services	225-379-1580	225-379-1853	joemodicut@dotd.state.la.us
Maine	John Dority, Chief Engineer	207-624-3000	207-624-3001	john.dority@maine.gov
Maryland	Douglas Rose, Deputy Administrator - Chief Engineer for Operations	410-545-0360	410-209-5010	drose@sha.state.md.us
Maryland	Joseph Geckle, Homeland Security Coordinator	301-952-0555 410-582-5552	301-952-1657 410-582-9861	jgeckle@sha.state.md.us
Maryland (2)	Russell A. Yurek, Director, Office of Maintenance	410-582-5055	410-582-9861	ryurek@sha.state.md.us
Massachusetts	Gordon Broz, Deputy Chief Engineer			Gordon.Broz@state.ma.us
Massachusetts	Kelly O'Neil	617-973-7745		Kelly.O'Neil@mhd.state.ma.us
Michigan	Eileen Phifer, Safety Administrator	517-373-1898	517-335-2765	phifere@michigan.gov
Michigan (2)	Tim Jones, Emergency Management Coordinator	517-241-2877	517-335-2787	jonesti@michigan.gov

Minnesota	Sonia Pitt, Homeland Security Planning Director	651-296-8895	651-402-1395	Sonia.Pitt@dot.state.mn.us
Mississippi	Bob Chapman, State Emergency Coordinator	601-359-7111	601-359-7126	bchapman@mdot.state.ms.us
Missouri	Scott Stotlemeyer, Technical Support Engineer	573-526-1759	573-526-4868	stotls@mail.modot.state.mo.us
Montana	Jim Hyatt	406-444-6152	406-444-7684	jhyatt@state.mt.us
Nebraska	Jim Schmailzl, Operations Manager	402-479-4787	402-479-4567	jschmail@dor.state.ne.us
Nevada	Frank G. Taylor, Chief Maintenance Engineer	775-888-7050	775-888-7211	ftaylor@dot.state.nv.us
Nevada	Alan Hilton, Research Division Chief	775-888-7803		ahilton@dot.state.nv.us
New Hampshire	Kenneth Kyle, Assistant Director of Operations	603-271-7419	603-271-3914	kkyle@dot.state.nh.us
New Jersey	Harold Neil, Executive Assistant 2	609-530-5309	609-530-3894	Harold.Neil@dot.state.nj.us
New Mexico	Deputy Secretary Rick Chavez, Security Liaison	505-827-5106	505-827-5115	Rick.Chavez@nmshtd.state.nm.us\
New York	Paul Gavin, Security Liaison	518-457-1043	518-457-5583	pgavin@dot.state.ny.us
North Carolina	Mrinway Biswas (TRB Rep)	919-715-2465	919-715-0137	biswas@dot.state.nc.us
North Dakota	Doug Faiman	701-328-2561	701-328-4545	dfaiman@state.nd.us
Ohio	Keith Swearingen, Administrator Office of Maintenance	614-466-3264	614-728-5590	keith.swearingen@dot.state.oh.us
Oklahoma	John Fuller, Assistant Director of Operations	405-521-4675		Jfuller@odot.org
Oregon	Rose Gentry, State Emergency Operations Manager	503-986-3020	503-986-3032	rosemary.m.gentry@odot.state.or.us
Pennsylvania	Daniel Leonard, P.E.	717-705-1448	717-705-0686	danleonard@state.pa.us
Puerto Rico	Aldio Alvarado-Torres, Security Office Director	787-728-9075	787-726-2442	alalvarado@act.dtop.gov.pr
Rhode Island	John D. Nickelson, Deputy Chief Engineer	401-222-2378 x4800	401-222-2940	jnick@dot.state.ri.us
South Carolina	Carl Chase, Assets Manager	803-737-1960	803-737-2038	chasec@scdot.org
South Dakota	David Huft	605-773-3292	605-773-4713	dave.huft@state.sd.us
Tennessee	Mike Shinn, Chief of Administration	615-741-5374	615-741-0865	Mike.Shinn@state.tn.us
Texas	J. Scott Alley, Emergency Management Coordinator	512-416-3187	512-416-2642	Jalley@dot.state.tx.us
Utah	Stan Burns (TRB Rep)	801-965-4196		sburns@utah.gov
Vermont	Alec Portalupi, Maintenance Programs Engineer	802-828-3889	802-828-2848	alec.portalupi@state.vt.us
Virginia	Steven Mondul, Security Management Division Administrator	804-786-2978		Steve.Mondul@VirginiaDOT.org
Washington	Terry Simmonds, Emergency Management Program Manager	360-705-7857	360-705-6823	SimmonT@wsdot.wa.gov
Washington (Research)	Rhonda Brooks, Research Manager for Design, Security, and Environmental Research	360-705-7370		BrooksR@wsdot.wa.gov
West Virginia	James L. Riggs, Emergency Coordinator	304-558-2901	304-558-2912	jriggs@dot.state.wv.us
Wisconsin	Jeff Western, Director of Infrastructure Security	608-264-8712	608-264-6667	jeffrey.western@dot.state.wi.us
Wyoming	Kenneth Shultz, State Maintenance Engineer	307-777-4458	307-777-4765	Ken.Shultz@dot.state.wy.us

Abbreviations used without definitions in TRB publications:

AASHO	American Association of State Highway Officials
AASHTO	American Association of State Highway and Transportation Officials
APTA	American Public Transportation Association
ASCE	American Society of Civil Engineers
ASME	American Society of Mechanical Engineers
ASTM	American Society for Testing and Materials
ATA	American Trucking Associations
CTAA	Community Transportation Association of America
CTBSSP	Commercial Truck and Bus Safety Synthesis Program
DHS	Department of Homeland Security
FAA	Federal Aviation Administration
FHWA	Federal Highway Administration
FMCSA	Federal Motor Carrier Safety Administration
FRA	Federal Railroad Administration
FTA	Federal Transit Administration
IEEE	Institute of Electrical and Electronics Engineers
ITE	Institute of Transportation Engineers
NCHRP	National Cooperative Highway Research Program
NCTRP	National Cooperative Transit Research and Development Program
NHTSA	National Highway Traffic Safety Administration
NTSB	National Transportation Safety Board
SAE	Society of Automotive Engineers
TCRP	Transit Cooperative Research Program
TRB	Transportation Research Board
TSA	Transportation Security Administration
U.S.DOT	United States Department of Transportation