FUSION CENTER INTEROPERABILITY: DATA DEFINITION AND CHARACTERIZATION

SOUTHEAST REGION RESEARCH INITIATIVE

FRANCES H. BUTLER
JANET S. MURRILL

MAY, 2008

Prepared for the
Department of Homeland Security

Budget Activity Number 4000052793

Prepared by the
Y-12 National Security Complex
Oak Ridge, TN 37831-8169
Managed by
B&W Y-12, L.L.C.
For the
U.S. DEPARTMENT OF ENERGY
Under contract DE-AC05-00OR22800

CAUTION

This document has not been given final patent clearance and is for internal use only. If this document is to be given public release, it must be cleared through the site Technical Information Office, which will see that the proper patent and technical information reviews are completed in accordance with B&W Y-12, L.L.C. policy.

This work of authorship and those incorporated herein were prepared by Contractor as accounts of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Contractor, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, use made, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency or Contractor thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency or Contractor thereof.

NOTICE: This document contains information of a preliminary nature. It is subject to revision or correction and therefore does not represent a final report.

CONTENTS

FIGURES

FUSION CENTER INTEROPERABILITY DATA DEFINITION AND CHARACTERIZATION

INTRODUCTION

The ability to share intelligence information quickly and accurately among state fusion centers and emergency operating centers (EOCs) is crucial in preventing potential criminal and terrorist acts and is recognized as a significant challenge by the current administration. In response to this challenge, President Bush issued in October 2007 the first *National Strategy for Information Sharing: Success and Challenges in Improving Terrorism-Related Information Sharing* to prioritize and unify our Nation's efforts to advance the sharing of terrorism-related information. The President stated "The *Strategy* will help ensure those responsible for combating terrorism and protecting our local communities have access to the timely and accurate information they need." He also stated that it is imperative that the legal rights of Americans continue to be protected especially in the area of privacy and civil liberties.

The objective of this project is to understand the data flow and constraints surrounding the Southeast Region Research Initiative (SERRI) Information Sharing and Management Projects (IS&MS) and their respective EOCs and state fusion centers.

The four SERRI information sharing projects are:

1. Shelby County Fusion Center (SCFC).

2. Data Sharing Middleware for Information Dissemination among Heterogeneous Sources.

3. Kentucky Intelligence Fusion Center Enhancement.

4. Kentucky Transportation Center (KTC) Integrated Threat Tracking and Information System (ITTIS).

DOCUMENT PURPOSE

This white paper will summarize the results of the project team's analysis and establish the following:

- a detailed description of each of the four IS&MS projects and the data associated with them,
- definitions of current data flows,
- an information sharing baseline including a comparison with current policies and/or requirements,
- a preliminary listing of policies,
- a critical data needs list, and
- current and future data needs.

A vital part of this document will be the inclusion of future recommendations. As the culmination of Phase I activities, these recommendations will be important inputs into the work scope for Phases II and III.

LANDSCAPE ASSESSMENT

An extensive Internet and document review was conducted to identify any policies and procedures in effect for governing intelligence data sharing among fusion centers and EOCs. Keywords searched are shown in Appendix B. Websites and documents examined are shown in Appendix C. Since fusion centers are relatively new and continuing to evolve, the landscape assessment did not discover consistent guidance or policies related to intelligence data sharing among the fusion centers and with other government and private entities. Information will continue to be monitored throughout the project to ensure new relevant information is taken into account.

In addition to the research described in the previous paragraph, the project team also participated in personal interviews with representative local, state, and Federal agencies shown in Figure 1. Figure 1 represents the local, state, and Federal law enforcement and emergency management facilities and organizations studied for this review. The figure illustrates the governmental hierarchy through which information must be communicated to ensure security of the homeland. Not only is vertical information flow essential (downward from DHS at the Federal level and upward from the first responder and local level), but horizontal information flow across functional areas (e.g., fusion centers and emergency operations) and across states (e.g., Tennessee and Kentucky) is equally important. Specifically, those organizational entities reviewed for this study are shown in Table 1.

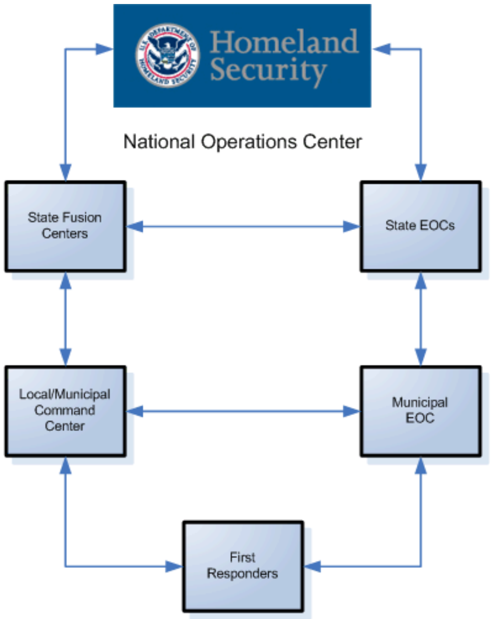

Figure 1. Law Enforcement and Emergency Management Organizational Entities

1. *Shelby County Sensor Fusion Center (SCFC)* – This project will incorporate near-real-time data visualization from two sensor systems: Port of Memphis and Sensor Network Area Protection System (SNAPS/SNAPSII), and will provide:
   - a computational platform for integrating sensor and data for use in decision making prior to, during, and after hazardous incidents in Shelby County, TN;
   - situational assessments in near real-time as well as gathering and sharing these assessments to multiple response agencies; and
   - near-real-time data visualization from the two sensor systems during deployments and plume model results.

   Figure 2 illustrates an overview of the system.

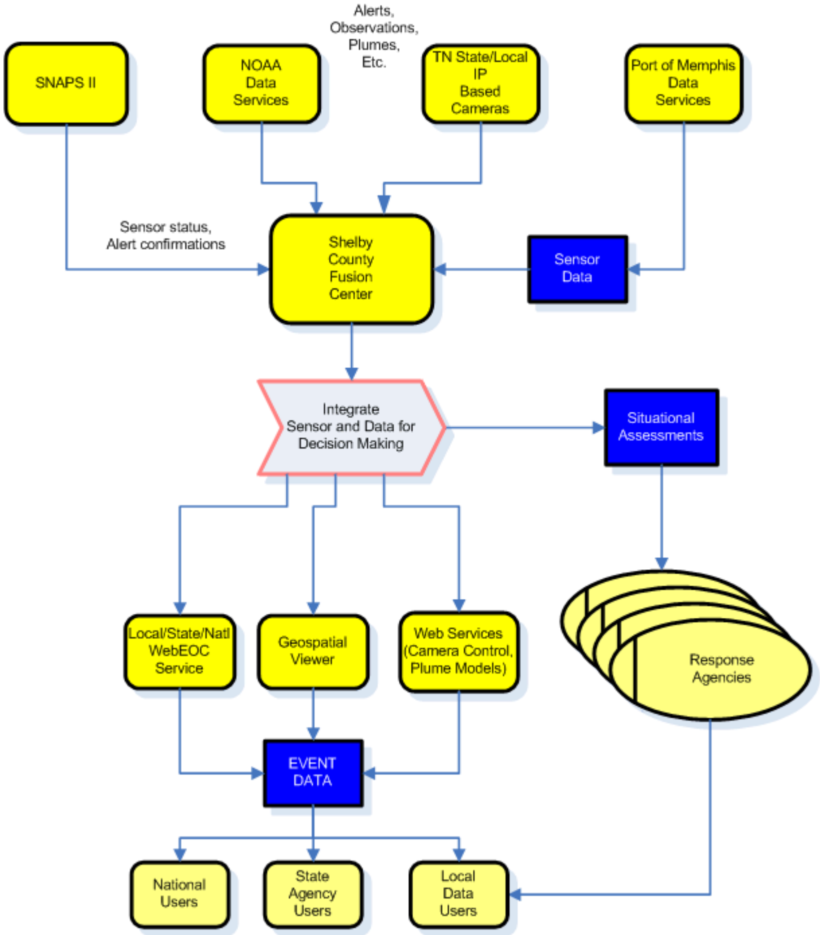
Alerts,
Observations,
Plumes,
Etc.
SNAPS II
NOAA Data Services
TN State/Local IP Based Cameras
Port of Memphis Data Services
Sensor status, Alert confirmations
Shelby County Fusion Center
Sensor Data
Integrate Sensor and Data for Decision Making
Situational Assessments
Local/State/Natl WebEOC Service
Geospatial Viewer
Web Services (Camera Control, Plume Models)
Response Agencies
EVENT DATA
National Users
State Agency Users
Local Data Users

Figure 2. SCFS Overview

2. *Data-Sharing Middleware for Information Disseminating among Heterogeneous Sources (INFO-D)*– A key growing need is to provide derived knowledge for empirical real-time situational awareness systems that span wide-area deployments (such as E911 systems in a metropolitan area). Information sharing among various agencies and emergency response teams requires delivery and display of accurate, time-sensitive data for rapid coordination and efficient operations. This project will develop a data sharing "middleware" that can handle multiple distributed data sources and dynamically changing data items, to assist in real-time information dissemination across multiple agencies for homeland security purposes. This will be used as an enabling technology that is able to "translate" data from different sources into a repository maintained with common templates so that data can be moved from originators to requestors in a generic manner. Figure 3 provides an overview of the technology components.

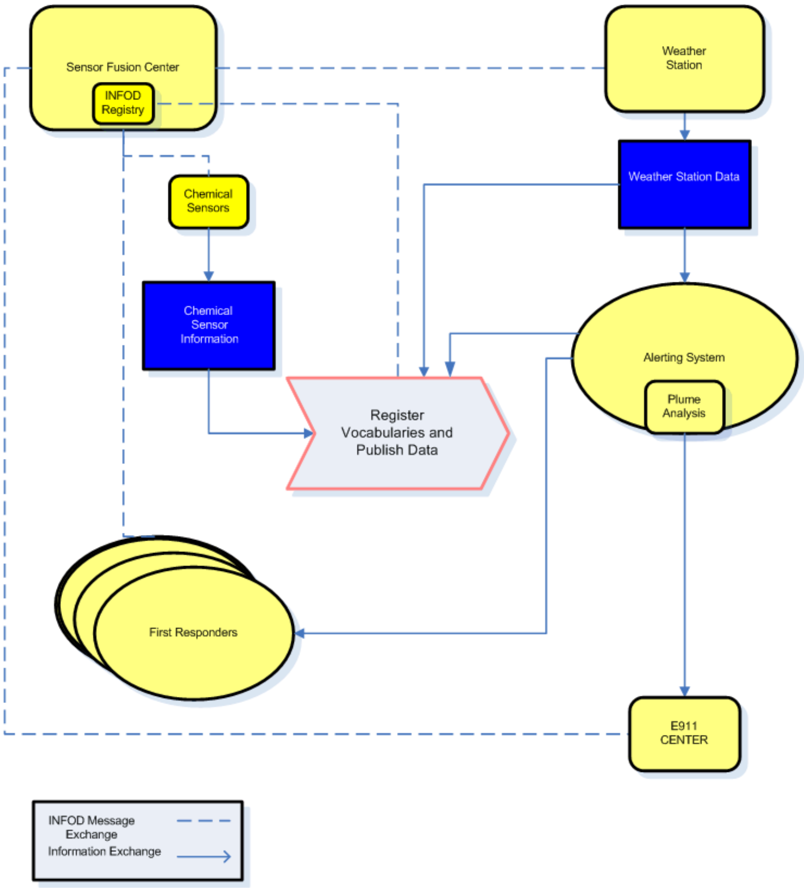

Figure 3. INFOD Overview

3. *Kentucky Intelligence Fusion Center (KIFC)* – The KIFC will employ a geographic information system (GIS) to include a map of Kentucky with the location of the fixed weigh stations and the current or last known position of the mobile systems indicated. The system will also include GIS Hazardous Shipment Displays, GIS Display of Infrastructure and Threat Group(s), GIS Reality Mobile Video and Tracking, and will provide for collaboration with NOC and other state Fusion Centers (e.g., Tennessee). An overview is shown in Figure 4 below.

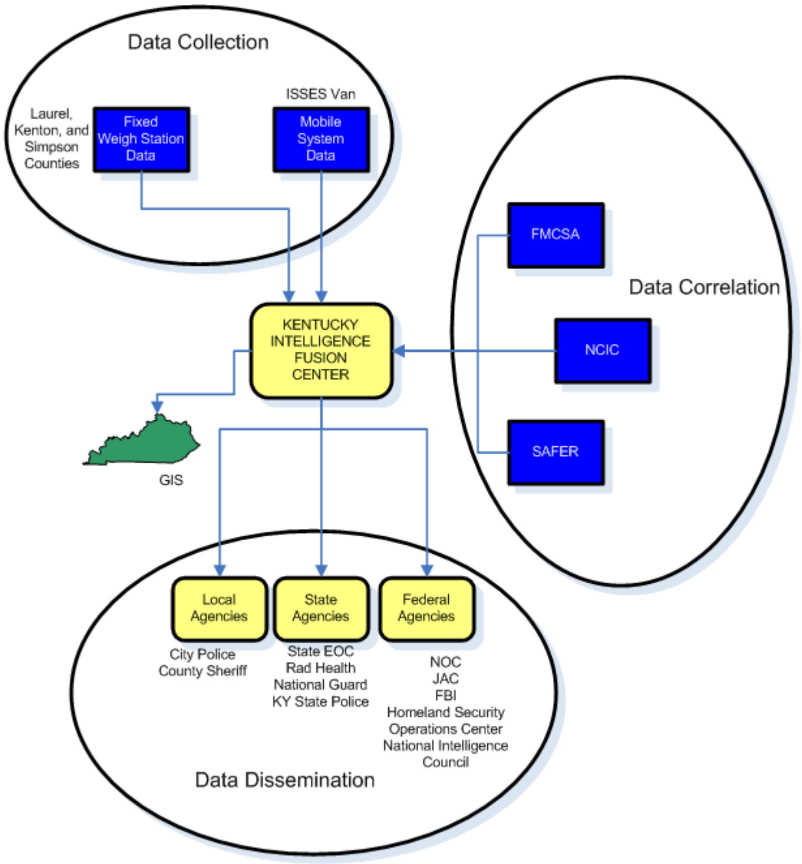

Figure 4. KIFC Overview

4. *Integrated Threat Tracking and Information System (ITTIS)* - This project provides an examination and assessment of the total homeland security threat profile for the Commonwealth of Kentucky and what information is required to interdict, plan, and perform consequence management. In addition, this project will develop a baseline system for real-time tracking of hazardous materials shipments on Kentucky's roadways. This project has two tasks: Threat Assessment and Hazmat Tracking.
   a. The Hazmat Tracking task will use electronic manifest data. This will include real-time transponder data which can identify the location of the vehicles which could be competitor-sensitive data. Trucking companies do not want their competitors to be able to view their routes. Other data elements that might be considered "sensitive" would be drivers' license numbers and certifications. Any data on the Hazmat manifest is public knowledge.
   b. Real-time alerts will be sent to the Kentucky Fusion Center for defined incidents, but the nature of those incidents has not yet been determined.
   c. A Conduct of Operations document and a system requirements/design document will be completed during the summer of 2008. This documentation will be reviewed by the Y-12 team once it becomes available, and its information will be factored into Phase II.

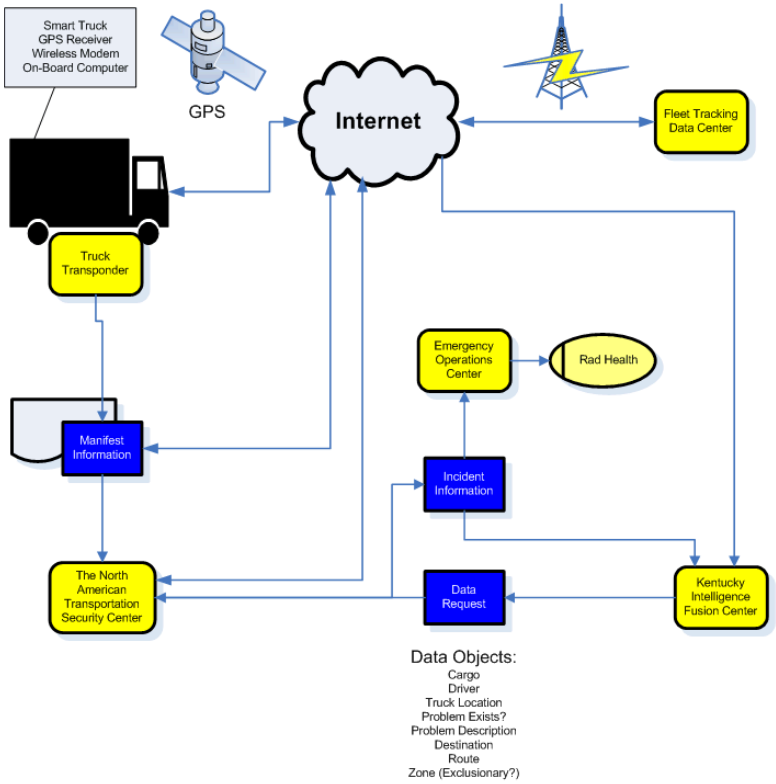

Figure 5. ITTIS Overview

DATA DEFINITION AND CHARACTERIZATION

The methodology used in this analysis included personal interviews as well as a review of available documentation. In addition to the four SERRI Information Sharing and Management Projects described earlier, the analysis team also gathered information from the Tennessee Fusion Center in Nashville, the FBI's Field Intelligence Group (FIG) in Memphis, and the Memphis Real Time Crime Center (RTCC). These facilities provided additional information relative to data requirements and also provided preliminary insight relative to the policy review in Phases II and III.

Subsequent to the interviews, a list of data objects was generated. This list is shown in Table 2 below.

ORGANIZATIONS AND INDIVIDUALS INTERVIEWED

Table 1 lists the organizational or information system entities as well as facilities included in the analysis. It should be noted that several organizations were included beyond representatives of the four projects described earlier in this document.

▪ *Table 1: Organizational Entities Included in Analysis.*

Entity	Entity Type	Organizational Tier	Governing Agency	POC/ Title
Integrated Threat Tracking and Information System (ITTIS)	Threat Assessment and Hazmat Tracking System	2	Kentucky Office of Homeland Security	Joe Crabtree, PhD University of Kentucky Kentucky Transportation Center
Shelby County Sensor Fusion Center	Local/Municipal Command Center	2	Shelby County Sheriff	Hamilton Hunter Oak Ridge National Laboratory
INFO-D	Data-Dissemination Middleware for Distributed Systems	1	University of Tennessee and Oak Ridge National Laboratory	Arjun Shankar, ORNL Researcher Daniel Getman, Oak Ridge National Laboratory
Kentucky Intelligence Fusion Center	GIS	3	Commonwealth of Kentucky Office of Homeland Security	Cyrus Smith Oak Ridge National Laboratory
Tennessee Fusion Center	State Fusion Center	3	Tennessee Bureau of Investigation (TBI), Governor's Office of Homeland Security State of Tennessee	Steven W. Hewitt, Supervisory Intelligence Officer
Tennessee Emergency Operations Center	State EOC	3	Tennessee Emergency Management Agency (TEMA)	Cecil Whaley, TEMA EOC Operations Director
Kentucky Emergency Operations Center	State EOC	3	Kentucky Emergency Management (KyEM)	Tony Keathley, Charlie Winter, Assistant Director

Entity	Entity Type	Organizational Tier	Governing Agency	POC/ Title
Kentucky Intelligence Fusion Center	State Fusion Center	3	Kentucky Office of Homeland Security	Shelby Lawson, Jr., Deputy Director of Operations and Prevention
Kentucky Event Mapping Analysis Portal (KEMAP)	Information System	3	Commonwealth of Kentucky Office of Technology	Kenny D. Ratliff, Dir., Division of Geographic Information
Memphis Field Office – Field Intelligence Group (FIG)	Federal	4	Federal Bureau of Investigation	William Carter
Shelby County Sensor Fusion Center	Local/Municipal Command Center	2	Shelby County Sheriff's Office	Captain Dale Lane Homeland Security Commander Special Operations Division
Memphis Urban Area Security Initiative	Local/Municipal Agency	2	Memphis Office of Homeland Security	Levell Blanchard, Deputy Director
Real Time Crime Center	Local/Municipal Command Center	2	Memphis Police Department	Major Jim Harvey

Results from the various interviews determined a critical data needs and data flow among law enforcement and emergency management organizational entities as illustrated in Figure 6 below.

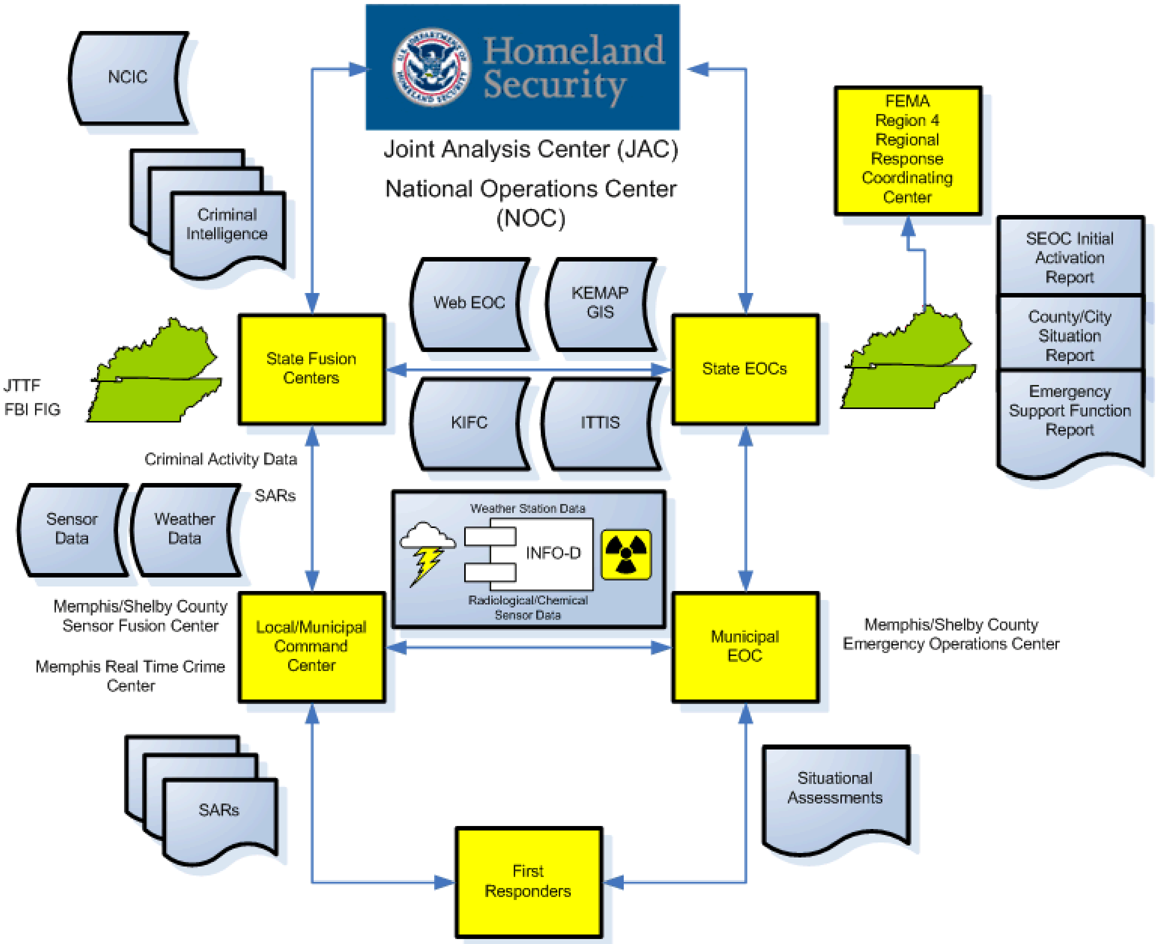
NCIC
Homeland Security
Joint Analysis Center (JAC)
National Operations Center (NOC)
FEMA Region 4 Regional Response Coordinating Center
Criminal Intelligence
SEOC Initial Activation Report
Web EOC
KEMAP GIS
County/City Situation Report
State Fusion Centers
State EOCs
JTTF
FBI FIG
KIFC
ITTIS
Emergency Support Function Report
Criminal Activity Data
SARs
Sensor Data
Weather Data
Weather Station Data
INFO-D
Radiological/Chemical Sensor Data
Memphis/Shelby County Sensor Fusion Center
Memphis Real Time Crime Center
Local/Municipal Command Center
Municipal EOC
Memphis/Shelby County Emergency Operations Center
SARs
Situational Assessments
First Responders

Figure 6. SERRI Project Data Flow

Critical data objects discerned from the analysis are listed in the table below.

▪ *Table 2: Data Objects.*

Object	Governing Agency/Source
Suspicious Activity Report (SAR)	TBI/Tennessee Fusion Center
Pre-Attack Indicator	TBI/Tennessee Fusion Center
Person>Criminal/Driver	TBI/Tennessee Fusion Center
Situational Assessment	Shelby County Sheriff/Shelby County Sensor Fusion Center
Vehicle>Truck/Auto	TBI/Tennessee Fusion Center
Relationship	TBI/Tennessee Fusion Center
Activity	TBI/Tennessee Fusion Center
Chemical and/or Radiological measurement	Shelby County Sensor Fusion Center
Weather data	Tennessee Emergency Management Agency (TEMA)
State Map (e.g., Kentucky, Tennessee)	Kentucky Office of Homeland Security

Object	Governing Agency/Source
Truck Manifest	Kentucky Office of Homeland Security
Vehicle Registration	Kentucky Office of Homeland Security
Vehicle License Plate	Kentucky Office of Homeland Security
Video Stream	Kentucky Office of Homeland Security
Radiation Situation	Kentucky Office of Homeland Security
Chemical Spill	Tennessee Emergency Management Agency (TEMA)
Terrorist Incident	Kentucky Office of Homeland Security

Legacy information systems reviewed in this analysis are listed in Table 3. Each of the systems in the table (with the exception of eGuardian, which is not yet operational) is currently being used by agencies at the state level (level 3 of the organizational hierarchy). This is noteworthy because a goal is to leverage existing databases, systems, and networks available via participating entities in order to maximize effective information sharing.

■ *Table 3: Information Sharing Systems*

Information System	Description	Sponsor/Governing Agency
eGuardian	**Coming summer 2008 –** A National Terrorism Information Sharing Tool on the desktop. It is intended for fusion centers and federal, state, local, and tribal law enforcement practitioners to provide, access, share, and use unclassified threat and incident data. Only system that allows law enforcement partners access to unclassified data from Guardian	FBI
Homeland Security Information Network (HSIN)	HSIN is a computer-based counterterrorism communications system connecting all 50 states, five territories, Washington, D.C., and 50 major urban areas. HSIN allows all states and major urban areas to collect and disseminate information between federal, state, and local agencies involved in combating terrorism. • helps provide situational awareness • facilitates information sharing and collaboration with homeland security partners throughout the federal, state and local levels • provides advanced analytic capabilities • enables real time sharing of threat information This communications capability delivers to states and major urban areas real-time interactive connectivity with the National Operations Center. This collaborative communications environment was developed by state and local authorities.	FBI

Information System	Description	Sponsor/Governing Agency
Homeland Security State & Local Intelligence Community of Interest (HS SLIC)	• Collaborative environment to include weekly threat teleconferences, semi-annual topical conferences at the Secret level, and a restricted portal on the HSIN for sharing homeland security information among Intelligence Analysts at the Federal, State & Local level. • Information exchanged at the controlled, unclassified information (CUI) level, to include Law Enforcement Sensitive (LES) information. • Current participants number more than 1250, with approximately 70 percent from 41 States, and the District of Columbia, and the remainder from the Federal community (as of 3/08).	DHS Office of Intelligence and Analysis
Law Enforcement Online (LEO)	LEO supports the FBI's ten priorities by providing cost-effective, time-critical national alerts and information sharing to first responders, law enforcement, and antiterrorism and intelligence agencies in support of the Global War on Terrorism. LEO is provided to members of the law enforcement community at no cost to their respective agencies. It is the mission of LEO to catalyze and enhance collaboration and information exchange across the FBI and mission partners with state-of-the-art commercial off-the-shelf communications services and tools, providing a user-friendly portal and software for communications and information exchange. LEO is a 7 days a week, 24 hours a day online (real-time), controlled-access communications and information sharing data repository. It provides an Internet accessible focal point for electronic Sensitive But Unclassified (SBU) communication and information sharing for the international, federal, state, local, and tribal law enforcement agencies. LEO also supports antiterrorism, intelligence, law enforcement, criminal justice, and public safety communities worldwide. Users anywhere in the world can communicate securely using LEO.	FBI
National Crime Information Center (NCIC)	A nationwide information system dedicated to serving and supporting criminal justice agencies – local, state, and federal – in their mission to uphold the law and protect the public.	FBI
National Law Enforcement Telecommunication System	A national federated model for sharing information for law enforcement and the first responder community to provide instant, secure and authorized access to information stored in databases in all 50 states as well as critical information in the federal government.	Department of Justice
Regional Information Sharing Systems Program Nationwide Network (RISSNET)	A nationwide program of regionally oriented services designed to enhance the ability of local, state, federal, and tribal criminal justice agencies to: • Identify, target, and remove criminal conspiracies and activities spanning multijurisdictional, multistate, and international boundaries. • Facilitate secure and rapid information sharing among law enforcement agencies pertaining to known suspected criminals or criminal activity. • Increase coordination and communication among agencies that are in pursuit of criminal conspiracies determined to be inter-jurisdictional.	Department of Justice

INFORMATION SHARING BASELINE AND POLICIES

A preliminary listing of policies identified in this analysis is shown below. The policies were prioritized into two categories: fundamental (i.e., primary) and secondary. Among the fundamental policies, the ones that govern privacy and/or civil liberties are arguably most important. Therefore, privacy and civil liberty policies will be the initial focus of future policy identification efforts.

A principal resource for the development of the preliminary policies was the *Fusion Center Guidelines,* developed as a collaborative effort between the U.S. Department of Justice (DOJ) and the U.S. Department of Homeland Security (DHS). Note that the policies range from stringent Federal law (code of Federal regulations) to recommended standards and/or guidelines. In addition to legal/statutory policies, technical standards or enabling technologies (e.g., Global JXDM) were also considered.

<u>Fundamental Policies:</u>

- 28 CFR
- National Criminal Intelligence Sharing Plan (NCISP) (provides collection limitations)
- Freedom of Information Act (FOIA)
- Fusion Center Privacy and civil liberties policies
- Applying Security Practices to Justice Information Sharing
- Homeland Security Information Act of 2002
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- The Family Education Rights and Privacy Act of 1974 (FERPA)

<u>Secondary Policies</u>:

- MOUs
- Non-Disclosure Agreements
- Personnel security clearances
- Law Enforcement Analytic Standards
- Fusion Center Personnel Training
- Develop, publish, and adhere to a policies and procedures manual
- Mission Statement/Goals

<u>Enabling Technologies:</u>

- Global Justice Extensible Markup Language (XML) Data Model (Global JXDM)
- Radio Frequency Identification (RFID) and supply chain systems
- Internet forms
- Business and messaging standards
- Service Oriented Architecture (SOA/XML/Web Services)
- Department of Transportation Intelligent Transportation Standards

Phase II of this project will validate the internal policies with the user organizations, and thereafter determine if additional policies/laws are associated with the data. Table 4 is an example of the data policy matrix anticipated during Phase II. The vertical axis lists the organizational entities reviewed and will include the critical data objects. The horizontal axis lists the laws and policies that would apply in each case. A checkmark is inserted to indicate where a given organization or data object intersects with a given policy.

■ *Table 4: Information Sharing Baseline and Policies.*

	Statute/Policy Jurisdiction			
	28 CFR	PUBLIC LAW 104-191: HIPAA	20 U.S.C. § 1232g; 34 CFR Part 99: FERPA	TN Code Annotated 58-2-101
	Federal Government	Federal Government	Federal Government	State of Tennessee
Organizational Entity				
Level 1 – First Responders				
Level 2 – Local/Municipal Command Centers/Municipal EOCs				
SCFC				
UASI – Memphis				
Real Time Crime Center Memphis PD			☑	
FBI FIG				
Level 3 – State Fusion Centers/State EOCs				
TN Fusion Center	☑	☑		
TN EOC				☑
KIFC				
KY Transportation Center				
Kentucky EOC				
Level 4 – Federal Agencies				

OBSERVATIONS/RECOMMENDATIONS

The observations identified during the first half of the project, listed below, can be grouped into three major categories:

1. Due to time constraints, insufficient information has been collected to date on tier one and tier four data. This is because the majority of the fusion center projects are integrated with tier 3 which limits a full and clear understanding of the present condition.

   Recommendation: The project team will continue to focus on collecting additional information during the second half of the project.

2. The Tennessee and Kentucky fusion centers do not have a privacy policy. State personnel are currently developing policy documents but are at different stages of completion.

   Recommendation: Provide assistance to Tennessee and Kentucky fusion centers by leveraging the state(s) that have already defined their privacy policy. This will facilitate the completion of this vital policy and will close this gap. When available, the project team will incorporate the policy into the final project analysis.

3. The intelligence analysis community expressed concern about information overload within fusion centers to varying degrees which have not been fully defined.

   Recommendation: The project team will continue analysis of this trend and assist in defining the overload and possible solutions.

Table 5 enumerates observations made during the analysis, provides recommendations on the scoping of Phase II and III, and comments on the extent of data flow not defined in Phase I.

▪ *Table 5: Information Sharing Baseline and Policies.*

Item Number	Observation	Recommendation
1	Other states cannot currently access Tennessee's incident reports from the Fusion Center in an automated fashion.	Employ data-sharing middleware (e.g., INFOD) to connect information systems between Tennessee and Kentucky.
2	State fusion centers do not currently have final, published Privacy Policies.	Review/analyze any existing privacy policies that may exist (*e.g.*, draft created by the University of Alabama at Huntsville) and tailor them to fulfill this requirement.
3	There is limited information sharing between state fusion centers and state EOCs.	Develop an understanding of the data sharing constraints and provide support to state fusion centers and/or state emergency operations centers in their data integration efforts.
4	It is not clear that local/municipal command centers are consistently sharing data with state fusion centers in their own state or with other states.	Investigate the systems and processes in place for efficient electronic file sharing, while ensuring privacy rights.
5	Due to time constraints, data requirements of the DHS Joint Analysis Center (JAC) and the National Operations Center (NOC) were not investigated during Phase I of this project.	Include data requirements from the Federal level of the organizational hierarchy.
6	Due to time constraints, data generated by first responders was not investigated during Phase I of this project.	Characterize data objects generated/provided by first responders such as county 911 centers, municipal ambulance services, and municipal fire departments.
7	State fusion centers receive large amounts of raw data from disparate sources that require expeditious analysis to create criminal intelligence.	Interview criminal intelligence analysts to fully understand their process of data analysis, perform a high-level landscape assessment of available automated tools, and then generate prospective alternative solutions to address their concerns.

PATH FORWARD

For project continuity, the team has listed the path forward from now through FY10. The primary focus during the remainder of FY08 will be to close the information gaps and initiate the policy constraint review. In addition, by providing assistance in leveraging the work completed thus far by the State of Alabama, a formal fusion center privacy policy will be completed.

The policy constraint review will be completed during FY09, when it is expected that several of the secondary policies will be formalized. In addition, FY09 will support an assessment of the tier three and other Southern Shield states and support defining solutions to two key issues facing the fusion centers: information overload and intrastate information sharing.

FY10 will bring the assessment of the remaining states within Southern Shield and support defining solutions to the final key issues facing the fusion centers: interstate information sharing. In addition, the team will support problem resolution based on the availability of funds.

The path forward rationale utilizes initial assessments as a solid landscape for understanding and placement of overarching constraints. The assessments also provide a mechanism to share lessons learned with the users or implementers. By permitting the team to provide assistance on in-depth constraint definition and resolution, the overall SERRI effort provides positive attributes back to DHS as a service:

1) Continuity of project team involvement,

2) Leverages DHS assets with state assets,

3) Permits DHS to provide assistance to solidifying Southern Shield, and

4) Problems identified are followed through to resolution.

FY08 Tasks

- Initiate Phases II and III
    - Fundamental policy review
    - Assess critical data against policy
- Address data gaps
    - Complete data flow understanding
    - Confirm observations
    - Define intelligence information overload
- Leverage Alabama written policy efforts to assist Tennessee and Kentucky
- Report results to Southern Shield

FY09 Tasks

- Complete Phases II and III
  - Secondary policy review
  - Assess critical data against policy
- Conduct tier 3 assessment on 4 states: Alabama, North Carolina, Virginia, Georgia
- Support problem/solution definition
  - Information overload
  - Intrastate information sharing
  - Interstate information sharing
- Report results to Southern Shield

FY10 Tasks

- Conduct tier 3 assessment on 3 states: Mississippi, South Carolina, Florida
- Support problem resolution
  - Information Overload Resolution
  - Intrastate information sharing
  - Interstate information sharing
- Report results to Southern Shield

APPENDIX A: ABBREVIATIONS, ACRONYMS, AND DEFINITIONS

28 CFR Part 23	A guideline for law enforcement agencies that operate federally funded multijurisdictional criminal intelligence systems.
FEMA	Federal Emergency Management Agency
Freedom of Information Act (FOIA)	The Freedom of Information Act, 5 U.S.C. 552, enacted in 1966, statutorily provides that any person has a right, enforceable in court, to access federal agency records, except to the extent that such records (or portions thereof) are protected from disclosure by one of nine exemptions.
DHS	Department of Homeland Security
DNDO	Domestic Nuclear Detection Office
DOT	Department of Transportation
EOC	Emergency Operation Center
FERPA	The Family Education Rights and Privacy Act of 1974 is a federal law that protects the privacy of student education records. Students have specific, protected rights regarding the release of such records and FERPA requires that institutions adhere strictly to these guidelines.
FIG	Field Intelligence Group
FMCSA	Federal Motor Carrier Safety Administration
GIS	Graphical Information System
GJXDM	Global Justice Extensible Markup Language Data Model
GPS	Global Positioning System
HIPAA	Health Insurance Portability and Accountability Act of 1996
HSIN	Homeland Security Information Network
ITTIS	Integrated Threat Tracking and Information System
JAC	Joint Analysis Center
JTTF	Joint Terrorism Task Force
KEMAP	Kentucky Event Mapping Analysis Portal

KIFC	Kentucky Intelligence Fusion Center
KTC	Kentucky Transportation Center
LEO	Law Enforcement Online
MOU	Memorandum of Understanding
National Criminal Intelligence Sharing Plan (NCISP)	A formal intelligence sharing initiative, supported by the U.S. Department of Justice that securely links local, state, tribal, and federal law enforcement agencies, facilitating the exchange of critical intelligence. The Plan contains model policies and standards and is a blueprint for law enforcement administrators to follow when enhancing or building an intelligence function. It describes a nationwide communications capability that will link all levels of law enforcement personnel, including officers on the street, intelligence analysts, unit commanders, and police executives.
NCIC	National Crime Information Center
NLETS	National Law Enforcement Telecommunication System
OHS	Office of Homeland Security
RFID	Radio Frequency Identification
RISSNET	Regional Information Sharing Systems Program Nationwide Network
RTCC	Real Time Crime Center
SAFER	Safety and Fitness Electronic Records System
SAR	Suspicious Activity Report
SCFC	Shelby County Fusion Center
SERRI	Southeast Region Research Initiative
SNAPS	Sensor Network Area Protection System
SOA	Service Oriented Architecture
TBI	Tennessee Bureau of Investigation
TDOC	Tennessee Department of Corrections
THP	Tennessee Highway Patrol
TNG	Tennessee National Guard

TEMA	Tennessee Emergency Management Agency
TRIC	Tennessee Regional Information Center
UASI	Urban Area Security Initiative
XML	Extensible Markup Language

APPENDIX B: KEYWORDS SEARCHED

Criminal intelligence information sharing
Fusion centers
Homeland security
Information privacy
Intelligence information sharing
Privacy policy
SERRI
Southeast Regional Research Initiative

APPENDIX C: REFERENCES

Applying Security Practices to Justice Information Sharing, March 2004, Version 2.0, www.it.ojp.gov/global.

Evaluation Checklists for Intelligence Units, Paul R. Roger

Executive Order 12291 28CFR, Part 23

Fusion Center Guidelines, Developing and Sharing Information in a New Era, Global Justice Information Sharing Initiative, http://it.ojp.gov/fusioncenterguidelines/intro.html

IACP National Law Enforcement Policy Center, Criminal Intelligence "Model Policy"

Criminal Intelligence File Guidelines, Law Enforcement Intelligence Unit, March 2002

Fusion Process Technical Assistance Program Resource Center, DHS Lessons Learned Information Sharing network (LLIS.gov)

The National Criminal Intelligence Sharing Plan, Global Justice Information Sharing Initiative, October 2003.

National Strategy for Information Sharing, October 2007.

Use of Technology in Intelligence Fusion Centers: An Oracle White Paper, April 2007.

Justice Information Privacy Guideline: Developing, Drafting and Assessing Privacy Policy for Justice Information Systems, September 2002, National Criminal Justice Association

Privacy Policy Development Guide, Global Justice Information Sharing Initiative, September 2006

What's Wrong with Fusion Centers?, ACLU, December 2007

Information Fusion Centers and Privacy, Electronic Privacy Information Center, http://epic.org/privacy/fusion/

Fusion Center Resources, Global Justice Information Sharing Initiative, Institute for Intergovernmental Research, http://www.iir.com/global/

Intelligence Sharing: Efforts to Develop Fusion Center Intelligence Standards, Peter A. Modafferi, Chair, IACP Police Investigative Operations Committee, and Chief of Detectives, Rockland Country District Attorney's Office, New City, NY, and Kenneth A. Bouche, Colonel, Illinois State Police, Springfield, IL, "The Police Chief", December 2005, http://policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article_id=514&issue_id=22005#2

Breaking Down Intelligence Barriers for Homeland Security, Dana R. Dillon, April 2002, http://www.heritage.org/Research/HomelandSecurity/BG1536.cfm

State Intelligence Fusion Centers: Recent State Actions, Joe Trella, NGA Center for Best Practices, September 2005, http://www.nga.org/files/pdf/0509fusion.pdf

Establishing State Intelligence Fusion Centers, Chris Logan, NGA Center for Best Practices, July 2005, http://www.nga.org/portal/site/nga/menuitem.9123e83a1f6786440ddcbeeb501010a0/?vgnextoid=560a6c6721115010VgnVCM1000001a01010aRCRD&vgnextchannel=4b18f074f0d9ff00VgnVCM1000001a01010aRCRD

State Fusion Center Processes and Procedures: Best Practices and Recommendations, John Rollins and Timothy Connors, Director, Center for Policing Terrorism, Manhattan Institute for Policy Research, September 2007, http://www.manhattan-institute.org/html/ptr_02.htm

Testimony of Hugo Teufel III, Chief Privacy Officer, before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, March 2007, http://www.dhs.gov/xabout/structure/gc_1182276006278.shtm

http://www.hsarpabaa.com/ for comparable policy identification projects/solicitations. (Homeland Security Advanced Research Projects Agency)

Fusion Centers: Leave 'Em to the States, Jim Harper, March 2007, CATO Institute, http://www.cato.org/tech/tk/070314-tk.html

A Summary of Fusion Centers: Core Issues and Options for Congress, Todd Masse and John Rollins, Congressional Research Service (CRS) Report for Congress, September 2007, http://assets.opencrs.com/rpts/RL34177_20070919.pdf

National Infrastructure Protection Plan, DHS, 2006, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

Information Sharing Environment Implementation Plan, Program Manager Information Sharing Environment, November 2006, http://www.ise.gov/docs/ISE-impplan-200611.pdf

State fusion centers struggle to produce useful info, study finds, John Moore, FCW.com, July 2007, http://www.fcw.com/online/news/103365-1.html

Program Manager, Information Sharing Environment website, http://www.ise.gov/index.htm

Privacy Policy Development Guide and Implementation Templates, October 2006, http://it.ojp.gov/documents/Privacy_Guide_Final.pdf

Global Privacy and Information Quality Working Group documents at http://it.ojp.gov/topic.jsp?topic_id=55