



FUSION CENTER INTEROPERABILITY:
DATA DEFINITION AND
CHARACTERIZATION
PHASE II REPORT

SOUTHEAST REGION RESEARCH INITIATIVE

FRANCES H. BUTLER
JANET S. MURRILL

JANUARY, 2009

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

INTRODUCTION.....	5
DOCUMENT PURPOSE.....	5
LANDSCAPE ASSESSMENT.....	6
PROJECT DESCRIPTIONS.....	6
DATA DEFINITION AND CHARACTERIZATION.....	11
ORGANIZATIONS AND INDIVIDUALS INTERVIEWED.....	14
INFORMATION SHARING BASELINE AND POLICIES.....	17
OBSERVATIONS/RECOMMENDATIONS.....	35
PATH FORWARD.....	37
APPENDIX A: ABBREVIATIONS, ACRONYMS, AND DEFINITIONS.....	39
APPENDIX B: KEYWORDS SEARCHED.....	42
APPENDIX C: REFERENCES.....	43
APPENDIX D: INFORMATION FLOW CHART.....	48

FIGURES

Figure 1. Law Enforcement and Emergency Management Organizational Entities	6
Figure 2. SCFS Overview	7
Figure 3. INFOD Overview	8
Figure 4. KIFC Overview.....	9
Figure 5. ITTIS Overview	10
Figure 6. Critical Data Object Model	12
Figure 7. SERRI Project Data Flow	15

TABLES

Table 1: Data Objects.	11
Table 2: Data Objects Associated With ISMS Projects.....	13
Table 3: Governing Entities Included in Analysis.....	14
Table 4: Information Sharing Systems	16
Table 5: Federal Intelligence-Related Laws.	18
Table 6: Executive Orders of Interest to the National Intelligence Community.....	22
Table 7: Information Sharing Baseline and Data Policy Matrix.....	23
Table 8. Sample Policy Rule Set	26
Table 9: Observations and Recommendations.	36

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 (ITIS).

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.

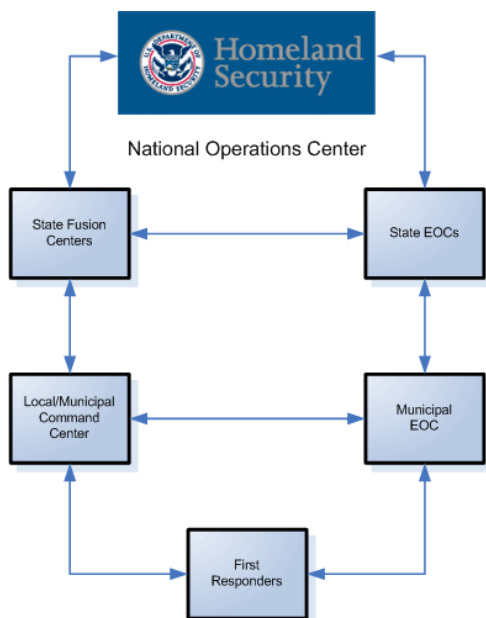


Figure 1. Law Enforcement and Emergency Management Organizational Entities

PROJECT DESCRIPTIONS

1. *Overview* – This section contains brief descriptions and graphical representations of the four SERRI projects included in the analysis. The figures are Event-Driven Process Chain (EPC) business process diagrams. The principal symbols commonly used in EPC diagrams are:

- Functions (rectangles), which are the basic building blocks of the diagram. Each function corresponds to an executed activity.
- Events (hexagons), which occur before and/or after a function is executed. Functions are linked by events, and
- Connectors (connecting lines), which associate activities and events.

In this report, the diagrams will also include ovals to symbolize organizational units, blue rectangles to designate data, and solid arrows to represent groups of processes.

2. *Shelby County Sensor Fusion Center (SCFC)* – This project incorporates near-real-time data visualization from two sensor systems: Port of Memphis and Sensor Network Area Protection System (SNAPS/SNAPSII), and provides:

- 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 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.

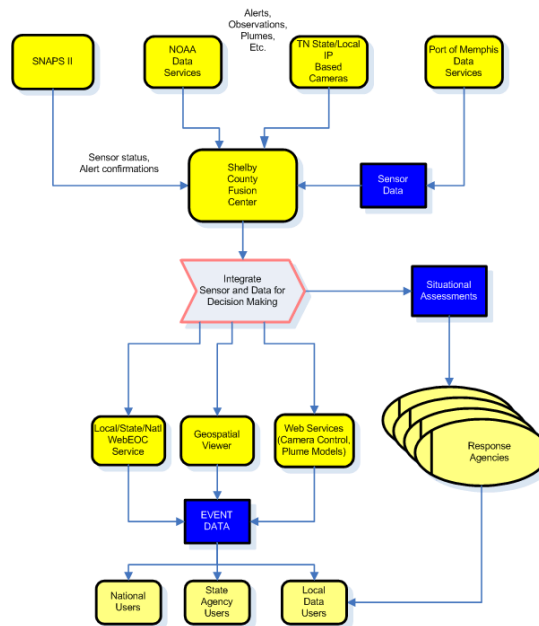


Figure 2. SCFS Overview

3. *Data-Sharing Middleware for Information Dissemination 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. INFO-D is 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 INFO-D technology components.

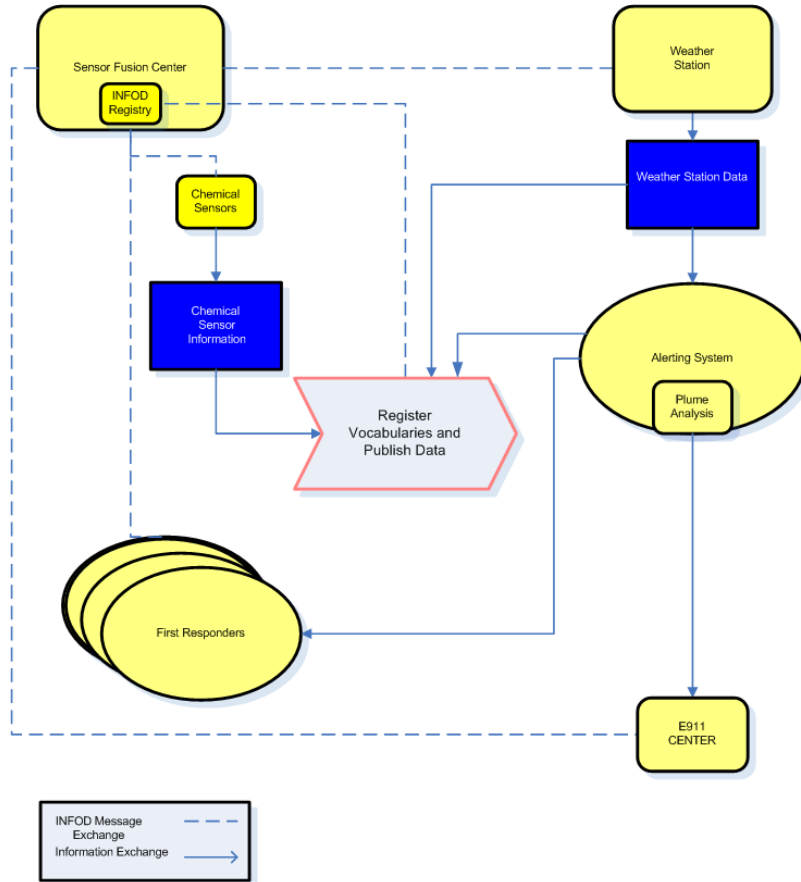


Figure 3. INFO-D Overview

4. *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.

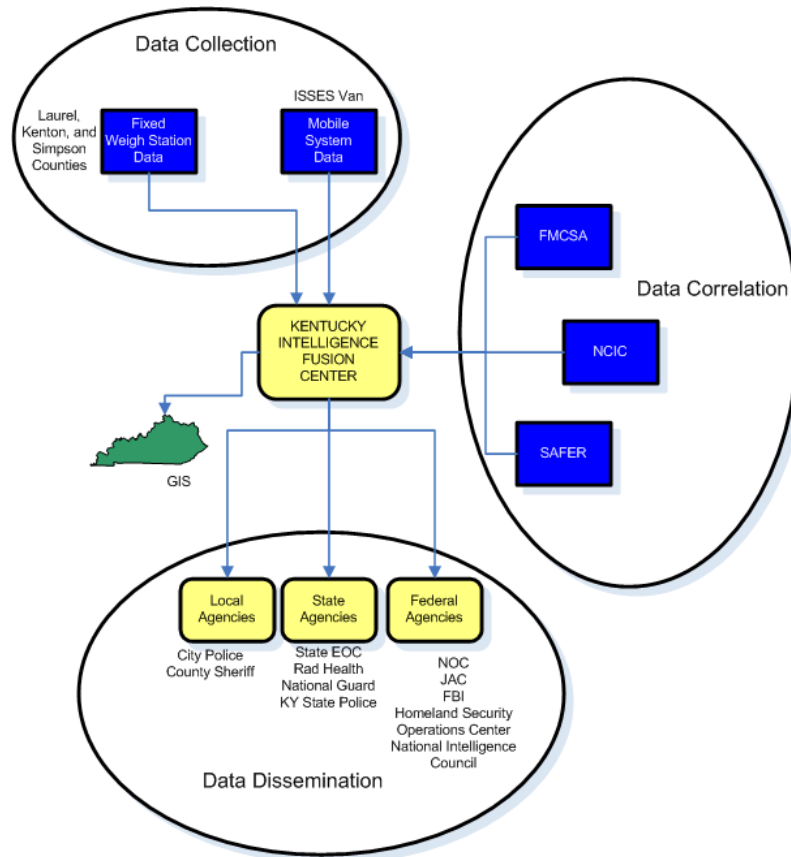


Figure 4. KIFC Overview

5. *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. During this phase of the project, draft conduct of operations and system requirements/design documentation relative to ITTIS was reviewed by the Y-12 team. In particular, the data objects contained in the U.S. Customs and Border Protection (CBP) Automated Commercial Environment (ACE) were factored in to the critical data objects list (Table 1).

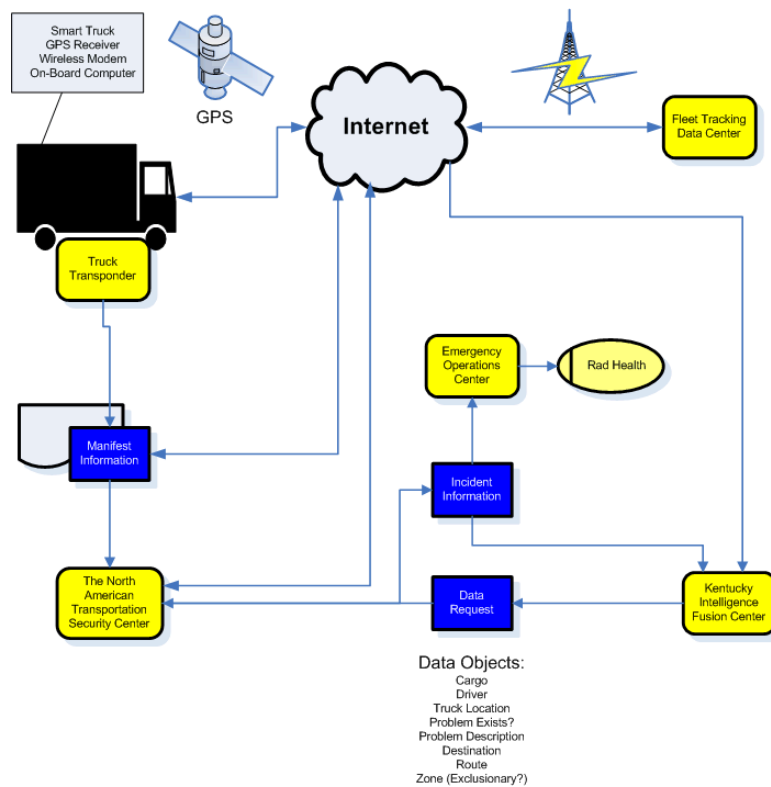


Figure 5. ITTIS Overview

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). Personnel at these facilities provided additional information relative to data requirements and also provided insight relative to the policy review. For example, the Family Education Rights and Privacy Act of 1974 (FERPA) was cited by RTCC personnel.

During and subsequent to the interviews, the “real world” (problem domain) critical objects were identified. The data objects, along with their sources, are listed in Table 1. Figure 6 illustrates those same data objects in the form of a static domain model. A domain is an area of knowledge or practice governed by distinct concepts and terminology. A domain model is a tool for communication, and is a representation only of real world conceptual objects, not of software components. Note that the source identification of each data object is included and the interrelationships among the data objects are shown.

■ Table 1: 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
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

Figure 6 is a Unified Modeling Language (UML) class diagram. The arrows indicate generalization or inheritance of data attributes (shown as an arrow with an “open” head). For example, the object “vehicle” is a data “supertype” that defines attributes for any vehicle. A real world vehicle has common attributes with any other vehicle (e.g., engine, steering wheel, etc.). Its subtypes are “truck” and “automobile.” While they share some attributes, trucks and automobiles each have unique attributes. Associations (relationships)

between classes are shown as connecting lines, and are also shown in Figure 6. The color-coded legend depicts the organizational entity that identified the data object during interviews.

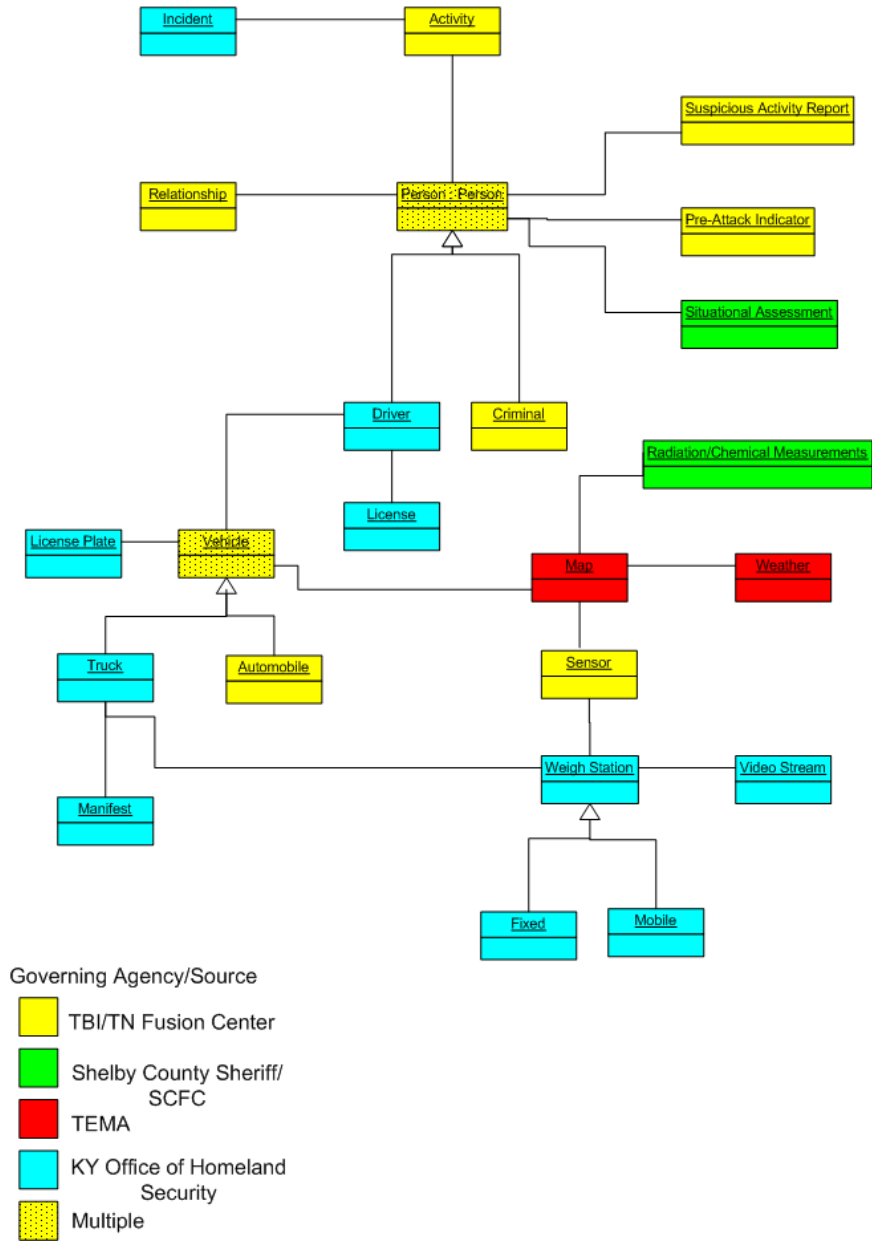


Figure 6. Critical Data Object Model

The next step in the analysis was to develop a matrix that associated the data objects with the ISMS project(s). Even though it was not one of the original “test case” projects, data objects identified by the Tennessee Fusion Center were also included. This was done because an understanding of the data requirements and transfer at state fusion centers is central to a thorough understanding of relevant policy. Table 2 provides a summary of the findings.

A detailed data requirements flow chart is provided in Appendix D and illustrates the data inputs, intelligence information products, and how the information is transferred among facilities, governing entities, and the four tiers in the organizational hierarchy. Note that horizontal interoperability (e.g., transfer of information from one first responder to another) as well as vertical transfer of information (one governmental tier to another) is shown on the diagram. Organizations, facilities, data systems, and data inputs/outputs are included. As this analysis was confined to two states (Tennessee and Kentucky), the vertical dashed line is shown to separate the information by state.

■ Table 2: Data Objects Associated With ISMS Projects.

	SCFC	INFO-D	KIFC	ITTIS	TN Fusion Center
Suspicious Activity Report (SAR)					●
Pre-Attack Indicator					●
Person					●
Driver’s License			●	●	
Situational Assessment	●				
Vehicle					●
Relationship					●
Activity					●
Weather Data		●			
State Map			●		
Vehicle Registration/License Plate			●	●	
Truck Manifest				●	
Video Stream	●		●		
Radiation/Chemical Measurements	●	●			
Incident	●		●	●	
Sensor Data	●		●		
Fixed Weigh Station Data			●		
Mobile System Data			●		
FMCSA			●		
NCIC			●		
SAFER			●		

ORGANIZATIONS AND INDIVIDUALS INTERVIEWED

Table 3 lists the governing or information system entities as well as facilities included in the analysis.

■ *Table 3: Governing Entities Included in Analysis.*

Entity	Entity Type	Organizational Tier	Governing Agency	POC/ Title
Integrated Threat Tracking and Information System (ITIS)	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	N/A	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
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

Entity	Entity Type	Organizational Tier	Governing Agency	POC/ Title
Real Time Crime Center	Local/Municipal Command Center	2	Memphis Police Department	Major Jim Harvey
Oak Ridge Fire Department	First Responder	1	City of Oak Ridge, TN	Chief Mack Bailey Captain Darrell Kerley

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 7.

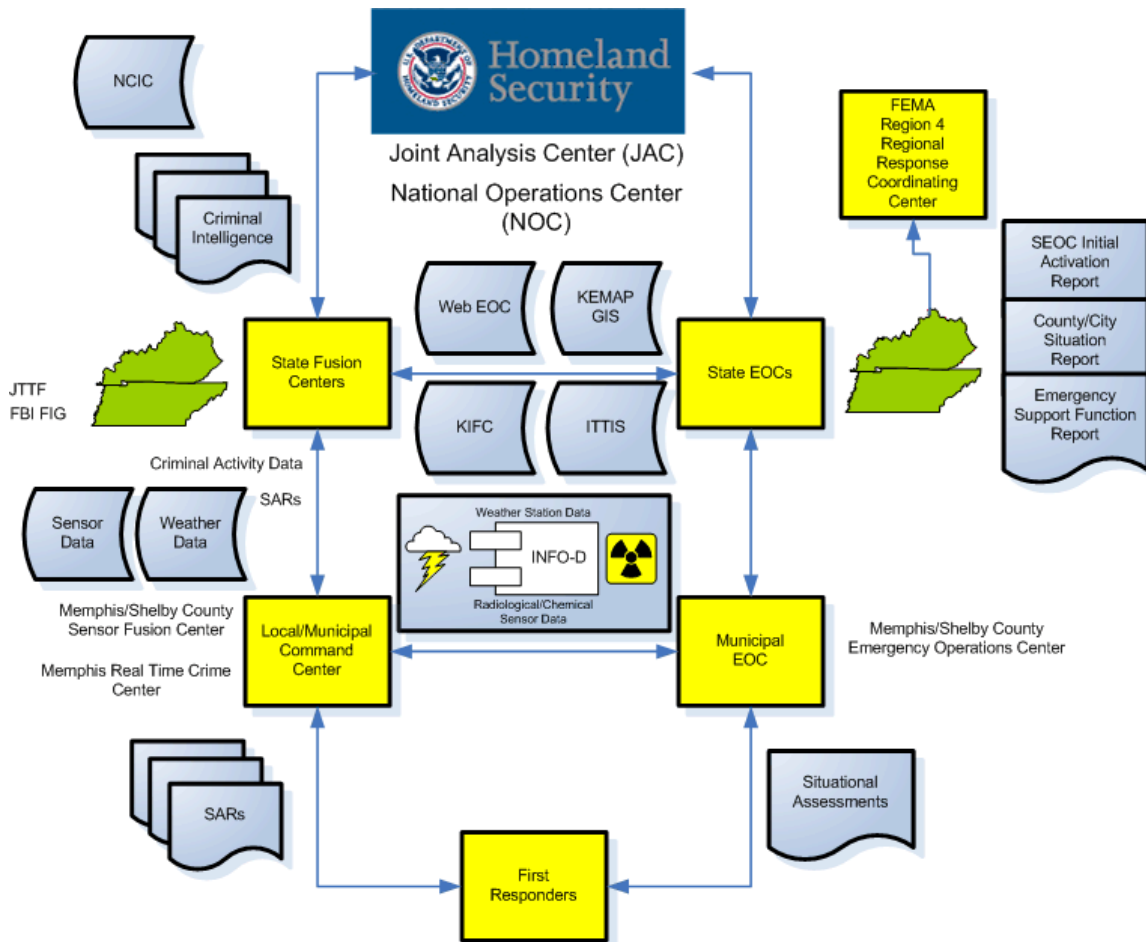


Figure 7. SERRI Project Data Flow

Legacy information systems reviewed in this analysis are listed in Table 3. Each of the systems in the table 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 4: Information Sharing Systems

Information System	Description	Sponsor/Governing Agency
eGuardian	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)	<p>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 among federal, state, and local agencies involved in combating terrorism.</p> <ul style="list-style-type: none"> • 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 <p>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.</p>	FBI
Homeland Security State & Local Intelligence Community of Interest (HS SLIC)	<ul style="list-style-type: none"> • 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 by providing time-critical national alerts and information sharing to first responders, law enforcement, and antiterrorism and intelligence agencies. LEO is provided to members of the law enforcement community at no cost to their respective agencies. LEO enhances collaboration and information exchange across the FBI and mission partners with state-of-the-art commercial off-the-shelf communications services and tools. It provides an Internet accessible focal point for electronic Sensitive But Unclassified (SBU) communication and information sharing for international, federal, state, local, and tribal law enforcement agencies. LEO also supports secure communications to antiterrorism, intelligence, law enforcement, criminal justice, and public safety communities worldwide.	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)	<p>A nationwide program of regionally oriented services designed to enhance the ability of local, state, federal, and tribal criminal justice agencies to:</p> <ul style="list-style-type: none"> • 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 listing of applicable 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.

Fundamental Policies:

- 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)
- The Privacy Act of 1974

Secondary Policies:

- 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

Enabling Technologies:

- National Information Exchange Model (NIEM)
- 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

Intelligence Oversight Laws:

During the mid-project review with Tennessee Fusion Center personnel, it was suggested that intelligence oversight laws be included with the compilation of relevant policies. A primary data source for such laws was the *Compilation of Intelligence Laws and Related Laws and Executive Orders of Interest to the National Intelligence Community*. This document was prepared for the use of the Permanent Select Committee on Intelligence of the House of Representatives. Selected public laws (as codified in the U.S. Code) related to intelligence oversight are listed in Table 4.

■ Table 5: Federal Intelligence-Related Laws.

Popular Name or Title	US Code Citation	Brief Description
Access to agency records by Comptroller General	31 USC § 716	Each agency shall give the Comptroller General information he/she requires about the duties, powers, activities, organization, and financial transactions of the agency. The Comptroller General may inspect an agency record to get the information.
Accountability for intelligence activities	50 USC § 413	Covers reports to Congressional Committees of intelligence activities and anticipated activities, reports concerning illegal intelligence activities, procedures for reporting information, procedures to protect from unauthorized disclosure, and defines “intelligence activities.”
Adjustment of status of certain non-immigrants to that of permanent resident alien	8 USC § 1255b	Allows for aliens (who are of good moral character and are admissible as permanent residents under the Immigration and Nationality Act) to become permanent residents so long as the Attorney General determines that it would be in the national interest, and that such action would not be contrary to the national welfare, safety, or security.
Assault on intelligence officers	18 USC § 1114	Provides for protection of officers and employees of the United States and outlines punishment for murder, manslaughter, or attempted murder or manslaughter according to definitions of statute.
Atomic Energy Act of 1954	42 USC § 2011 et seq., Chapters 2, 12, and 18	Protection of atomic energy (classified) information.
Classified Information Procedures Act (CIPA)	18 USC App. III. § 1-16.	The procedural protections of CIPA protect unnecessary disclosure of classified information. But CIPA does not restrict admissibility of classified information; rather, it simply enables the government to ascertain prior to trial the specific classified information which the defendant possesses, or seeks to admit at trial, so that the government can evaluate the effect of disclosure on national security. CIPA, by its terms, covers only criminal cases.

Popular Name or Title	US Code Citation	Brief Description
		CIPA only applies when classified information is involved, as defined in the Act's Section 1.
Communications Act of 1934	47 USC § 605	Prohibits unauthorized publication or use of communications.
Communications Assistance for Law Enforcement	47 USC §§ 1001-1010	Covers interception of digital and other communications.
Computer Security Act of 1987	40 USC 25 § 1441	Provides for a computer standards program within the National Bureau of Standards, to provide for Government-wide computer security, and provides for training in security matters of persons who are involved in the management, operation, and use of Federal computer systems, and for other purposes.
Congressional Investigations	2 USC §§ 192-94	Addresses the refusal of witness to testify or produce papers, privilege of witnesses, and certification of failure to testify or produce; grand jury action.
Counterintelligence access to telephone toll and transactional records	18 USC § 2709	A wire or electronic service provider must provide subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession in response to a request by the Director of the Federal Bureau of Investigation (FBI) if the Director of the FBI, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge designated by the FBI Director in a field office, certifies that the records or information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a U.S. person is not conducted solely on the basis of First Amendment protected activities.
Detection and monitoring of aerial and maritime transit of illegal drugs	10 USC § 124	Designates the Department of Defense as the single lead agency of the Federal Government for the detection and monitoring of aerial and maritime transit of illegal drugs into the United States. This responsibility shall be carried out in support of the counter-drug activities of Federal, State, local, and foreign law enforcement agencies.
Diplomatic codes and correspondence	18 USC § 952	Provides for fines and/or imprisonment for the willful publishing or transfer of any official diplomatic code or any matter prepared in such code.
Espionage, censorship, and venue	Chapter 37 of title 18, United States Code and 18 USC Sec. 3239	The trial for any offense involving a violation, begun or committed upon the high seas or elsewhere out of the jurisdiction of any particular State or district, may be in the District of Columbia or in any other district authorized by law.
Foreign Intelligence Surveillance Act of 1978 (FISA)	50 USC § 1801 et seq.	Prescribes procedures for requesting judicial authorization for electronic surveillance and physical search of persons engaged in espionage or international terrorism against the United States on behalf of a foreign power.

Popular Name or Title	US Code Citation	Brief Description
Freedom of Information Act (FOIA)	5 USC § 552	This act allows for the full or partial disclosure of previously unreleased information and documents controlled by the United States Government. The Act defines agency records subject to disclosure, outlines mandatory disclosure procedures and grants nine exemptions to the statute.
Homeland Security Act of 2002	6 USC § 121	This title concerns the responsibilities of the Department of Homeland Security for information analysis and infrastructure protection.
Immigration and Nationality Act	SEC. 101. [8 U.S.C. 1101] SEC. 102. [8 U.S.C. 1102] SEC. 105. [8 U.S.C. 1105] SEC. 207. [8 U.S.C. 1157] SEC. 212. [8 U.S.C. 1182] SEC. 215. [8 U.S.C. 1185] SEC. 222. [8 U.S.C. 1202] SEC. 235. [8 U.S.C. 1225] SEC. 241. [8 U.S.C. 1231] SEC. 244. [8 U.S.C. 1254a] SEC. 261. [8 USC 1301] SEC. 262. [8 USC 1302] SEC. 263. [8 USC 1303] SEC. 264. [8 USC 1304] SEC. 277. [8 USC 1327] SEC. 290. [8 USC 1360] SEC. 313. [8 USC 1424] SEC. 316. [8 USC 1427] SEC. 331. [8 USC 1442] SEC. 349. [8 USC 1481]	Covers liaison with internal security officers and data exchange, annual admission of refugees and admission of emergency situation refugees, general classes of aliens ineligible to receive visas and ineligible for admission; waivers of inadmissibility, travel documentation of aliens and citizens, issuance of entry documents; inspection, apprehension, examination, exclusion, and removal.
Intelligence Identities Protection Act of 1982	50 USC § 421–426	Makes it a federal crime to intentionally reveal the identity of an agent whom one knows to be in or recently in certain covert roles with a U.S. intelligence agency.
Internal Security Act (also known as the Subversive Activities Control Act, McCarran Act, or ISA) of 1950	SEC. 4. [50 USC 783]	Prohibits the unauthorized sharing of classified information by government employees, and also prohibits foreign agents or members of a Communist organization to receive classified information. It provides for fines and/or imprisonment for convicted violations.
Military Cooperation With Civilian Law Enforcement Agencies Act	10 USC §§ 8, 18, 141, 148	Allows the military of the United States to cooperate with law enforcement agencies in their operations, including (among others) drug interdiction.
National Narcotics Leadership Act of 1988 (Anti-Drug Abuse Act of 1988)	SEC. 1001. [21 USC 1501 nt] Title I and Secs. 4801, 6483, 7605	Established the Office of National Drug Control Policy (ONDCP) to develop and coordinate the policies and objectives of the federal government's program for reducing the use of illicit drugs.
Obstruction of correspondence and delay or destruction of mail or newspapers	18 USC §§ 1702-03	Provides for fines and/or imprisonment for tampering with the mails.
Privacy Act of 1974	5 USC § 552a	The Privacy Act states in part: No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another

Popular Name or Title	US Code Citation	Brief Description
		<p>agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains....</p> <p>There are specific exceptions for the record allowing the use of personal records:</p> <ul style="list-style-type: none"> • For statistical purposes by the Census Bureau and the Bureau of Labor Statistics • For routine uses within a U.S. government agency • For archival purposes "as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government" • For law enforcement purposes • For congressional investigations • Other administrative purposes <p>The Privacy Act mandates that each United States Government agency have in place an administrative and physical security system to prevent the unauthorized release of personal records.</p>
Right to Financial Privacy Act of 1978	12 USC 3401 et seq.	Congress' response to a U.S. Supreme Court decision that found bank customers had no legal right of privacy for their financial information held by financial institutions. The law is largely procedural and requires government agencies to provide notice and an opportunity to object before a bank or other institution can disclose personal financial information to a government agency, usually for law enforcement purposes. The law was amended in the latter 1980s to allow postponement of notice in investigations dealing with drug trafficking and espionage.
Securities Exchange Act of 1934	SEC. 13. [15 USC 78m] (a)	Reporting requirements and national security exemption: Section 13(b)(3)(A) of the Securities Exchange Act of 1934 provides that "with respect to matters concerning the national security of the United States," the President or the head of an Executive Branch agency may exempt companies from certain critical legal obligations. These obligations include keeping accurate "books, records, and accounts" and maintaining "a system of internal accounting controls sufficient" to ensure the propriety of financial transactions and the preparation of financial statements in compliance with "generally accepted accounting principles."
Testimonial immunity	18 USC §§ 6002, 6005	Deals with immunity before a court or grand jury of the US, or an agency of the US, or either House of Congress in Congressional proceedings.

Popular Name or Title	US Code Citation	Brief Description
USA Patriot Act	Sec. 203 Guidelines Sec. 905(a) Guidelines Sec. 905(b) Guidelines	The purpose of the USA PATRIOT Act is to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and other purposes. Sec. 203. Authority to share criminal investigative information. Sec. 905. Disclosure to Director of Central Intelligence of foreign intelligence-related information with respect to criminal investigations.

Selected Executive Orders, which constitute direction from the President on how executive agencies are to be managed, are listed in Table 5.

■ *Table 6: Executive Orders of Interest to the National Intelligence Community.*

Number	Title
EO 10450	Security Requirements for Government Employment
EO 12139	Exercise of Certain Authority Respecting Electronic Surveillance
EO 12537	President's Foreign Intelligence Advisory Board
EO 12333	United States Intelligence Activities
EO 12334	President's Intelligence Oversight Board
EO 12356	National Security Information
EO 12863	President's Foreign Intelligence Advisory Board
EO 12958	Classified National Security Information
EO 12968	Access to Classified Information
EO 13284	Amendment of Executive Orders, and Other Actions, in Connection With the Establishment of the Department of Homeland Security
EO 13292	Further Amendment to Executive Order 12958, as Amended, Classified National Security Information
EO 13311	Homeland Security Information Sharing
EO 13353	Establishing the President's Board on Safeguarding Americans' Civil Liberties
EO 13356	Strengthening the Sharing of Terrorism Information to Protect Americans
EO 13388	Further Strengthening the Sharing of Terrorism Information to Protect Americans
EO 13392	Improving Agency Disclosure of Information

Applicable State Laws:

The Tennessee Code Annotated and Kentucky Revised Statutes relevant to privacy were identified and are listed in Table 7.

The intent of Phase II of this project was to validate the internal policies with the user organizations, and to determine if additional policies/laws are associated with the data. Table 7 is the data policy matrix populated with available information to date. 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 7: Information Sharing Baseline and Data Policy Matrix.

	Level 2 – Local/ Municipal Command Centers/ Municipal EOCs Shelby County Sensor Fusion Center	Data Sharing Middleware INFO-D	Level 3 – State Fusion Centers/ State EOCs KIFC	Level 3 – State Fusion Centers/ State EOCs ITTIS	Level 3 – State Fusion Centers/ State EOCs Tennessee Fusion Center
Statute/Policy Jurisdiction					
US Constitution					
<ul style="list-style-type: none"> First Amendment Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances. 					
<ul style="list-style-type: none"> Fourth Amendment The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. 					
<ul style="list-style-type: none"> Sixth Amendment In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the state and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the assistance of counsel for his defense. 					
US Code					
Criminal Intelligence Systems Operating Policies 28 CFR Part 23	☑	☑	☑	☑	

	Level 2 – Local/ Municipal Command Centers/ Municipal EOCs Shelby County Sensor Fusion Center	Data Sharing Middleware INFO-D	Level 3 – State Fusion Centers/ State EOCs KIFC	Level 3 – State Fusion Centers/ State EOCs ITTIS	Level 3 – State Fusion Centers/ State EOCs Tennessee Fusion Center
Freedom of Information Act (FOIA) 5 USC § 552	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Health Insurance Portability and Accountability Act (HIPAA) PUBLIC LAW 104-191	<input checked="" type="checkbox"/>				
The Family Education Rights and Privacy Act of 1974 (FERPA) 20 U.S.C. § 1232g; 34 CFR Part 99	<input checked="" type="checkbox"/>				
The Privacy Act of 1974 5 USC § 552a	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Executive Orders					
10450 Security Requirements for Government Employment					
12139 Exercise of Certain Authority Respecting Electronic Surveillance					
12333 United States Intelligence Activities					
12334 President’s Intelligence Oversight Board					
12356 National Security Information					
12537 President’s Foreign Intelligence Advisory Board					
12863 President’s Foreign Intelligence Advisory Board					
12958 Classified National Security Information					
12968 Access to Classified Information					
13284 Amendment of Executive Orders, and Other Actions, in Connection With the Establishment of the Department of Homeland Security					
13292 Further Amendment to Executive Order					
13311 Homeland Security Information Sharing					
13353 Establishing the President’s Board on Safeguarding Americans’ Civil Liberties					
13355 Strengthened Management of the Intelligence Community					
13388 Further Strengthening the Sharing of Terrorism Information to Protect Americans					
Tennessee Code Annotated (TCA)					
Arrest and Conviction Records • TCA 40-31-101 • TCA 40-15-106					<input checked="" type="checkbox"/>
Credit Reporting and Investigations • TCA 47-22-104					
Criminal Justice Information Systems					<input checked="" type="checkbox"/>

	Level 2 – Local/ Municipal Command Centers/ Municipal EOCs Shelby County Sensor Fusion Center	Data Sharing Middleware INFO-D	Level 3 – State Fusion Centers/ State EOCs KIFC	Level 3 – State Fusion Centers/ State EOCs ITTIS	Level 3 – State Fusion Centers/ State EOCs Tennessee Fusion Center
• TCA 10-7-504					
Employment Records					
• TCA 8-50-108					
Library Records					
• TCA 10-8-101					
Medical Records					
• TCA 53-1322					
• TCA 10-7-504					
• TCA 24-1-207					
• TCA 63-117					
Privacy Statutes/State Constitutions	<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>
• TCA 47-25-1101-1108					
Privileged Communications					
• TCA 62-143					
• TCA 24-1-206					
Social Security Numbers	<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>
• TCA 55-50-331					
• TCA 4-4-125					
Student Records					
• TCA 10-7-504					
Kentucky Revised Statutes (KRS)					
Arrest and Conviction Records			<input checked="" type="checkbox"/>		
• KRS 61.884					
Computer Crime					
• KRS 434.840					
Credit					
• KRS 367.363-.367					
Criminal Justice			<input checked="" type="checkbox"/>		
• KRS 17.150					
Electronic Surveillance					
• KRS 526.010					
• KRS 531.100 and 110					
Government Information					
• KRS 61.870					
• KRS 61.878					
• KRS 61.884					
Identity Theft					
• KRS 514.160					
Medical					
• KRS 216.2927					

	Level 2 – Local/ Municipal Command Centers/ Municipal EOCs Shelby County Sensor Fusion Center	Data Sharing Middleware INFO-D	Level 3 – State Fusion Centers/ State EOCs KIFC	Level 3 – State Fusion Centers/ State EOCs ITTIS	Level 3 – State Fusion Centers/ State EOCs Tennessee Fusion Center
Privacy Statutes • KRS 61.872 – 61.884 • KRS 160.100 – 160.730 • KRS 391.170					
Social Security Numbers • KRS 186.412(2) and (3) • KRS 213.046(14) • KRS 156.160 • KRS 197.120 • KRS 18A.0551 • KRS 186.412 • KRS 402.100					
Student Records • KRS 156.160 • KRS 197.120					
Tax Records • KRS 131.190					
Telephone Services • KRS 367.46951 • KRS 367.461					

Once the appropriate policies are identified, each one is reviewed for applicable information sharing rules using a set of predefined keywords. These terms are used to highlight policy rules that can be interpreted by an automated information system. Table 8 lists an example using a sample subset of available and applicable policies.

■ Table 8. Sample Policy Rule Set

Popular Name	Citation	Rule Description
Freedom of Information Act	5 USC 552	Each agency, in accordance with published rules, shall make available for public inspection and copying-- (A) final opinions, including concurring and dissenting opinions, as well as orders, made in the adjudication of cases; (B) those statements of policy and interpretations which have been adopted by the agency and are not published in the Federal Register; (C) administrative staff manuals and instructions to staff that affect a member of the public; (D) copies of all records, regardless of form or format, which have been released to any person under paragraph (3) and which, because of the nature of their subject matter, the agency determines have become or are likely to become the subject of subsequent requests for substantially the same records; and (E) a general index of the records referred to under subparagraph (D);

Popular Name	Citation	Rule Description
Freedom of Information Act	5 USC 552	(3)(A) Except with respect to the records made available under paragraphs (1) and (2) of this subsection, and except as provided in subparagraph (E), each agency, upon any request for records which (i) reasonably describes such records and (ii) is made in accordance with published rules stating the time, place, fees (if any), and procedures to be followed, shall make the records promptly available to any person.
		In making any record available to a person under this paragraph, an agency shall provide the record in any form or format requested by the person if the record is readily reproducible by the agency in that form or format. Each agency shall make reasonable efforts to maintain its records in forms or formats that are reproducible for purposes of this section.
		In responding under this paragraph to a request for records, an agency shall make reasonable efforts to search for the records in electronic form or format, except when such efforts would significantly interfere with the operation of the agency's automated information system.
		An agency, or part of an agency, that is an element of the intelligence community (as that term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4))) shall not make any record available under this paragraph to-- (i) any government entity, other than a State, territory, commonwealth, or district of the United States, or any subdivision thereof; or (ii) a representative of a government entity described in clause (i).
		Each agency, upon any request for records made under paragraph (1), (2), or (3) of this subsection, shall--(i) determine within 20 days (excepting Saturdays, Sundays, and legal public holidays) after the receipt of any such request whether to comply with such request and shall immediately notify the person making such request of such determination and the reasons therefor, and of the right of such person to appeal to the head of the agency any adverse determination; and (ii) make a determination with respect to any appeal within twenty days (excepting Saturdays, Sundays, and legal public holidays) after the receipt of such appeal. If on appeal the denial of the request for records is in whole or in part upheld, the agency shall notify the person making such request of the provisions for judicial review of that determination under paragraph (4) of this subsection.
		This section does not apply to matters that are-- (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order.
		This section does not apply to matters that are related solely to the internal personnel rules and practices of an agency.
		This section does not apply to matters that are specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld
		This section does not apply to matters that are trade secrets and commercial or financial information obtained from a person and privileged or confidential.
		This section does not apply to matters that are inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency.

Popular Name	Citation	Rule Description
Freedom of Information Act	5 USC 552	This section does not apply to matters that are personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.
		This section does not apply to matters that are records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual.
		This section does not apply to matters that are contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions.
		This section does not apply to matters that are geological and geophysical information and data, including maps, concerning wells.
		Whenever a request is made which involves access to records described in subsection (b)(7)(A) and-- (A) the investigation or proceeding involves a possible violation of criminal law; and (B) there is reason to believe that (i) the subject of the investigation or proceeding is not aware of its pendency, and (ii) disclosure of the existence of the records could reasonably be expected to interfere with enforcement proceedings, the agency may, during only such time as that circumstance continues, treat the records as not subject to the requirements of this section.
		Whenever informant records maintained by a criminal law enforcement agency under an informant's name or personal identifier are requested by a third party according to the informant's name or personal identifier, the agency may treat the records as not subject to the requirements of this section unless the informant's status as an informant has been officially confirmed.
		Whenever a request is made which involves access to records maintained by the Federal Bureau of Investigation pertaining to foreign intelligence or counterintelligence, or international terrorism, and the existence of the records is classified information as provided in subsection (b)(1), the Bureau may, as long as the existence of the records remains classified information, treat the records as not subject to the requirements of this section.

Popular Name	Citation	Rule Description
Freedom of Information Act	5 USC 552	Each agency shall separately state and currently publish in the Federal Register for the guidance of the public-- (A) descriptions of its central and field organization and the established places at which, the employees (and in the case of a uniformed service, the members) from whom, and the methods whereby, the public may obtain information, make submittals or requests, or obtain decisions; (B) statements of the general course and method by which its functions are channeled and determined, including the nature and requirements of all formal and informal procedures available; (C) rules of procedure, descriptions of forms available or the places at which forms may be obtained, and instructions as to the scope and contents of all papers, reports, or examinations; (D) substantive rules of general applicability adopted as authorized by law, and statements of general policy or interpretations of general applicability formulated and adopted by the agency; and (E) each amendment, revision, or repeal of the foregoing.
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	PL 104-191	WRONGFUL DISCLOSURE OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION SEC. 1177. (a) OFFENSE. A person who knowingly and in violation of this part (1) uses or causes to be used a unique health identifier; (2) obtains individually identifiable health information relating to an individual; or (3) discloses individually identifiable health information to another person, shall be punished as provided in subsection (b). (b) PENALTIES. A person described in subsection (a) shall (1) be fined not more than \$50,000, imprisoned not more than 1 year, or both; (2) if the offense is committed under false pretenses, be fined not more than \$100,000, imprisoned not more than 5 years, or both; and (3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than \$250,000, imprisoned not more than 10 years, or both.
Privacy Act of 1974	5 USC 552a	Conditions of Disclosure.--No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be--(1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties; (2) required under section 552 of this title; (3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section; (4) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13; (5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable; (6) to the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value; (7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought; (8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual; (9) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee; (10) to the Comptroller General, or any of his authorized

Popular Name	Citation	Rule Description
		representatives, in the course of the performance of the duties of the Government Accountability Office; (11) pursuant to the order of a court of competent jurisdiction; or (12) to a consumer reporting agency in accordance with section 3711(e) of title 31.
Privacy Act of 1974	5 USC 552a	Accounting of Certain Disclosures. -Each agency, with respect to each system of records under its control, shall-- (1) except for disclosures made under subsections (b)(1) or (b)(2) of this section, keep an accurate accounting of: (A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection (b) of this section; and (B) the name and address of the person or agency to whom the disclosure is made; (2) retain the accounting made under paragraph (1) of this subsection for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made; (3) except for disclosures made under subsection (b)(7) of this section, make the accounting made under paragraph (1) of this subsection available to the individual named in the record at his request; and (4) inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of this section of any record that has been disclosed to the person or agency if an accounting of the disclosure was made.
		Each agency that maintains a system of records shall upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence.
		Each agency that maintains a system of records shall permit the individual to request amendment of a record pertaining to him and-- (A) not later than 10 days (excluding Saturdays, Sundays, and legal public holidays) after the date of receipt of such request, acknowledge in writing such receipt; and (B) promptly, either-- (i) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or (ii) inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review of that refusal by the head of the agency or an officer designated by the head of the agency, and the name and business address of that official.
		Each agency that maintains a system of records shall permit the individual who disagrees with the refusal of the agency to amend his record to request a review of such refusal, and not later than 30 days (excluding Saturdays, Sundays, and legal public holidays) from the date on which the individual requests such review, complete such review and make a final determination unless, for good cause shown, the head of the agency extends such 30-day period; and if, after his review, the reviewing official also refuses to amend the record in accordance with the request, permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement with the refusal of the agency, and notify the individual of the provisions for judicial review of the reviewing official's determination.

Popular Name	Citation	Rule Description
Privacy Act of 1974	5 USC 552a	In any disclosure, containing information about which the individual has filed a statement of disagreement, occurring after the filing of the statement under paragraph (3) of this subsection, clearly note any portion of the record which is disputed and provide copies of the statement and, if the agency deems it appropriate, copies of a concise statement of the reasons of the agency for not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed.
		Each agency that maintains a system of records shall maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive order of the President.
		Each agency that maintains a system of records shall collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs.
		Each agency that maintains a system of records shall inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual-- (A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary; (B) the principal purpose or purposes for which the information is intended to be used; (C) the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and (D) the effects on him, if any, of not providing all or any part of the requested information.
The Family Education Rights and Privacy Act of 1974 (FERPA)	20 U.S.C. § 1232g; 34 CFR Part 99	Personal information shall only be transferred to a third party on the condition that such party will not permit any other party to have access to such information without the written consent of the parents of the student. If a third party outside the educational agency or institution permits access to information in violation of paragraph (2)(A), or fails to destroy information in violation of paragraph (1)(F), the educational agency or institution shall be prohibited from permitting access to information from education records to that third party for a period of not less than five years.
Criminal Intelligence Systems Operating Policies	28 CFR Part 23	A project shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.
Criminal Intelligence Systems Operating Policies	28 CFR Part 23	A project shall not collect or maintain criminal intelligence information about the political, religious or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.

Popular Name	Citation	Rule Description
Criminal Intelligence Systems Operating Policies	28 CFR Part 23	Reasonable Suspicion or Criminal Predicate is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise. In an inter-jurisdictional intelligence system, the project is responsible for establishing the existence of reasonable suspicion of criminal activity either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.
		A project shall not include in any criminal intelligence system information which has been obtained in violation of any applicable Federal, State, or local law or ordinance. In an inter-jurisdictional intelligence system, the project is responsible for establishing that no information is entered in violation of Federal, State, or local laws, either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.
		A project or authorized recipient shall disseminate criminal intelligence information only where there is a need to know and a right to know the information in the performance of a law enforcement activity.
		Except as noted in paragraph (f)(2) of this section, a project shall disseminate criminal intelligence information only to law enforcement authorities who shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination which are consistent with these principles.
		Paragraph (f)(1) of this section shall not limit the dissemination of an assessment of criminal intelligence information to a government official or to any other individual, when necessary, to avoid imminent danger to life or property.
		A project maintaining criminal intelligence information shall ensure that administrative, technical, and physical safeguards (including audit trails) are adopted to insure against unauthorized access and against intentional or unintentional damage. A record indicating who has been given information, the reason for release of the information, and the date of each dissemination outside the project shall be kept. Information shall be labeled to indicate levels of sensitivity, levels of confidence, and the identity of submitting agencies and control officials. Each project must establish written definitions for the need to know and right to know standards for dissemination to other agencies as provided in paragraph (e) of this section. The project is responsible for establishing the existence of an inquirer's need to know and right to know the information being requested either through inquiry or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.
		Where appropriate, projects must adopt effective and technologically advanced computer software and hardware designs to prevent unauthorized access to the information contained in the system
		The project must restrict access to its facilities, operating environment and documentation to organizations and personnel authorized by the project.
		The project must store information in the system in a manner such that it cannot be modified, destroyed, accessed, or purged without authorization.

Popular Name	Citation	Rule Description
Criminal Intelligence Systems Operating Policies	28 CFR Part 23	The project must institute procedures to protect criminal intelligence information from unauthorized access, theft, sabotage, fire, flood, or other natural or manmade disaster.
		The project must promulgate rules and regulations based on good cause for implementing its authority to screen, reject for employment, transfer, or remove personnel authorized to have direct access to the system.
		A project may authorize and utilize remote (off-premises) system data bases to the extent that they comply with these security requirements.
		All projects shall adopt procedures to assure that all information which is retained by a project has relevancy and importance. Such procedures shall provide for the periodic review of information and the destruction of any information which is misleading, obsolete or otherwise unreliable and shall require that any recipient agencies be advised of such changes which involve errors or corrections. All information retained as a result of this review must reflect the name of the reviewer, date of review and explanation of decision to retain. Information retained in the system must be reviewed and validated for continuing compliance with system submission criteria before the expiration of its retention period, which in no event shall be longer than five (5) years.
		A project shall notify the grantor agency prior to initiation of formal information exchange procedures with any Federal, State, regional, or other information systems not indicated in the grant documents as initially approved at time of award.
		A project shall make assurances that there will be no purchase or use in the course of the project of any electronic, mechanical, or other device for surveillance purposes that is in violation of the provisions of the Electronic Communications Privacy Act of 1986, Public Law 99-508, 18 U.S.C. 2510-2520, 2701-2709 and 3121-3125, or any applicable State statute related to wiretapping and surveillance.
		A project shall make assurances that there will be no harassment or interference with any lawful political activities as part of the intelligence operation.
		A project shall adopt sanctions for unauthorized access, utilization, or disclosure of information contained in the system.
		A participating agency of an inter-jurisdictional intelligence system must maintain in its agency files information which documents each submission to the system and supports compliance with project entry criteria. Participating agency files supporting system submissions must be made available for reasonable audit and inspection by project representatives. Project representatives will conduct participating agency inspection and audit in such a manner so as to protect the confidentiality and sensitivity of participating agency intelligence records.
		The Attorney General or designee may waive, in whole or in part, the applicability of a particular requirement or requirements contained in this part with respect to a criminal intelligence system, or for a class of submitters or users of such system, upon a clear and convincing showing that such waiver would enhance the collection, maintenance or dissemination of information in the criminal intelligence system, while ensuring that such system would not be utilized in violation of the privacy and constitutional rights of individuals or any applicable state or federal law.

Popular Name	Citation	Rule Description
Criminal Intelligence Systems Operating Policies	28 CFR Part 23	These policy standards are applicable to all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, et seq., as amended.

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 and funding constraints, limited 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 three 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 remainder of the project.

2. The Tennessee and Kentucky fusion centers do not have a published 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 9 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 9: Observations and Recommendations.

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 National Operations Center (NOC) were investigated using one source of information: the NOC Mission Blueprint, during Phase I of this project.	Include data requirements from the Federal level of the organizational hierarchy as appropriate.
6	Due to time constraints, limited data generated by first responders was 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, this document includes the path forward from now through FY10. The primary focus during the remainder of FY09 will be to close any identified information gaps and to complete the policy constraint review by having personnel from the Tennessee Fusion Center to validate and/or comment upon the findings. In addition, by providing assistance in leveraging the work completed thus far by the State of Alabama, a model 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 upon 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.

First and Second Quarter FY09 Tasks

- Address data gaps
 - Complete data flow understanding
 - Confirm observations
- Complete Current Tasking
 - Finalize Report from Policy Study
 - Assess critical data against policy
- Leverage Alabama written policy efforts to assist TN and KY
- Develop Model Interstate Privacy Policy
- Continue Collaborative Efforts with University of Alabama-Huntsville
- Report results to Southern Shield

Third and Fourth Quarter FY09 Tasks

- Complete Phase III
 - Secondary policy review
 - Assess critical data against policy
- Develop User Identity Metadata Compliant with GFIPM
- Coordinate Policy Issues with MSSSI Task
- Support HSIN to Share Lessons Learned
- EOC/FC Training Course for Emergency Management Personnel
- Report results to Southern Shield

FY10 Tasks

- Continue Coordination of Policy Issues with MSSSI Task
- Continue HSIN support to share lessons learned
- Report results to Southern Shield

APPENDIX A: ABBREVIATIONS, ACRONYMS, AND DEFINITIONS

ACRONYM	DEFINITION
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
EPC	Event-Driven Process Chain
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
FOIA	Freedom of Information Act
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

ACRONYM	DEFINITION
JAC	Joint Analysis Center
JTTF	Joint Terrorism Task Force
KEMAP	Kentucky Event Mapping Analysis Portal
KIFC	Kentucky Intelligence Fusion Center
KRS	Kentucky Revised Statute(s)
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
Project	Organizational unit which operates an intelligence system on behalf of and for the benefit of a single agency or the organization which operates an inter-jurisdictional intelligence system on behalf of a group of participating agencies.
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

ACRONYM	DEFINITION
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
TCA	Tennessee Code Annotated
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
UML	Unified Modeling Language
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

Alabama Fusion Center (AFC) Privacy Policy: Privacy, Civil Rights, and Civil Liberties Policy, June 19, 2008.

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

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

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

Compilation of Intelligence Laws and Related Laws and Executive Orders of Interest to the National Intelligence Community As Amended through March 25, 3003, (Prepared for the Use of the Permanent Select Committee on Intelligence of the House of Representatives) June 2003.

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

Establishing State Intelligence Fusion Centers, Chris Logan, NGA Center for Best Practices, July 2005,
<http://www.nga.org/portal/site/nga/menuitem.9123e83a1f6786440ddcbceb501010a0/?vgnnextoid=560a6c6721115010VgnVCM1000001a01010aRCRD&vgnnextchannel=4b18f074f0d9ff00VgnVCM100001a01010aRCRD>

Evaluation Checklists for Intelligence Units, Paul R. Roger

Executive Orders: <http://www.archives.gov/federal-register/executive-orders/>

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

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

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

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

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

IACP National Law Enforcement Policy Center, Criminal Intelligence “Model Policy”

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

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

Intelligence Sharing: Efforts to Develop Fusion Center Intelligence Standards, Peter A. Modafferi, Chair, IACP Police Investigative Operations Committee, and Chief of Detectives, Rockland County 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

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

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

National Strategy for Information Sharing, October 2007.

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

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

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

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

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

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>

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

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

United States Code: <http://www.gpoaccess.gov/USCODE/index.html>

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

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

APPENDIX D: INFORMATION FLOW CHART

