SERRI Report 89900-01

Final Report: Multistate Sharing Initiative

SERRI Project: Information Sharing Framework & Development

Project Principal Investigators:
Edmon Begoli
Frank DeNap
Thomas Brant Boehmann

This material is based upon work supported by the U.S. Department of Homeland Security under U.S. Department of Energy Interagency Agreement 43WT10301. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.

SERRI Report 89900-01

SERRI Project: Information Sharing Framework & Development

FINAL REPORT: MULTISTATE SHARING INITIATIVE

Edmon Begoli
Frank DeNap
Oak Ridge National Laboratory

Thomas Brant Boehmann
Cadre5, LLC

Edited by: Cyrus Smith

Date Published:
October 2011

Prepared for
U.S. Department of Homeland Security
under U.S. Department of Energy Interagency Agreement 43WT10301

Prepared by
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, Tennessee 37831-6283
managed by
UT-BATTELLE, LLC
for the
U.S. DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22725

ACKNOWLEDGEMENTS

The authors would like to thank the Southeast Region Research Initiative for providing funding for this research and development program. Additionally, we would like to thank the states of Tennessee, South Carolina, and Alabama and the commonwealth of Kentucky for their participation in this effort.

CONTENTS

FIGURES

ABBREVIATIONS, ACRONYMS, AND INITIALISMS

API	application programming interface
CFR	Code of Federal Regulations
DHS	Department of Homeland Security
EconoSAR	Economy SAR System
IP	Internet protocol
MSSI	Multistate Sharing Initiative
NIEM	National Information Exchange Model
NSI	Nationwide Suspicious Activity Reporting Initiative
ORNL	Oak Ridge National Laboratory
PDF	Portable Document Format
SAR	Suspicious Activity Report
SERRI	Southeast Region Research Initiative
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
WSDL	Web Services Description Language
XML	Extensible Markup Language

SOUTHEAST REGION RESEARCH INITIATIVE

In 2006, the U.S. Department of Homeland Security commissioned UT-Battelle at the Oak Ridge National Laboratory (ORNL) to establish and manage a program to develop regional systems and solutions to address homeland security issues that can have national implications. The project, called the Southeast Region Research Initiative (SERRI), is intended to combine science and technology with validated operational approaches to address regionally unique requirements and suggest regional solutions with potential national implications. As a principal activity, SERRI will sponsor university research directed toward important homeland security problems of regional and national interest.

SERRI's regional approach capitalizes on the inherent power resident in the southeastern United States. The project partners, ORNL, the Y-12 National Security Complex, the Savannah River National Laboratory, and a host of regional research universities and industrial partners, are all tightly linked to the full spectrum of regional and national research universities and organizations, thus providing a gateway to cutting-edge science and technology unmatched by any other homeland security organization.

As part of its mission, SERRI supports technology transfer and implementation of innovations based upon SERRI-sponsored research to ensure research results are transitioned to useful products and services available to homeland security responders and practitioners.

For more information on SERRI, go to the SERRI Web site: www.serri.org.

EXECUTIVE SUMMARY

In 2003 a joint effort between the U.S. Department of Homeland Security (DHS) and the U.S. Department of Justice created state and metropolitan intelligence fusion centers. These fusion centers were an effort to share law enforcement, disaster, and terrorism related information and intelligence between state and local jurisdictions and to share terrorism related intelligence between state and local law enforcement agencies and various federal entities.

In 2006, DHS commissioned the Oak Ridge National Laboratory to establish and manage a groundbreaking program to assist local, state, and tribal leaders in developing the tools and methods required to anticipate and forestall terrorist events and to enhance disaster response. This program, called the Southeast Region Research Initiative (SERRI), combines science and technology with validated operational approaches to address regionally unique requirements and suggest regional solutions with the potential for national application.

In 2009, SERRI sponsored the Multistate Sharing Initiative (MSSI) to assist state and metropolitan intelligence fusion centers with sharing information related to a wider variety of state interests than just terrorism. While these fusion centers have been effective at sharing data across organizations within their respective jurisdictions, their organizational structure makes bilateral communication with federal entities convenient and also allows information to be further disbursed to other local entities when appropriate. The MSSI-developed Suspicious Activity Report (SAR) sharing system allows state-to-state sharing of non-terrorism-related law enforcement and disaster information.

Currently, the MSSI SAR system is deployed in Alabama, Kentucky, Tennessee, and South Carolina. About 1 year after implementation, cognizant fusion center personnel from each state were contacted to ascertain the status of their MSSI SAR systems. The overwhelming response from these individuals was that the MSSI SAR system was an outstanding success and contributed greatly to the security and resiliency of their states. At least one state commented that SERRI's implementation of the MSSI SAR actually "jump started" and accelerated deployment and acceptance of the Nationwide Suspicious Activity Reporting Initiative (NSI).

While all states were enthusiastic about their systems, South Carolina and Tennessee appeared to be the heaviest users of their respective systems. With NSI taking the load of sharing SARs with other states, Tennessee has redeployed the MSSI SAR system within Tennessee to allow SAR sharing between state and local organizations including Tennessee's three Homeland Security Regions, eleven Homeland Security Districts, and more than 500 police and sheriff offices, as well as with other states. In one success story from South Carolina, the Economy SAR System was used to compile similar SARs from throughout the state which were then forwarded to field liaison officers, emergency management personnel, and law enforcement officers for action.

1. BACKGROUND

In 2003 a joint effort between the U.S. Department of Homeland Security (DHS) and the U.S. Department of Justice created state and metropolitan intelligence fusion centers. These fusion centers were an effort to enhance sharing of law enforcement, disaster, and terrorism related information and intelligence between state and local jurisdictions and sharing of terrorism related intelligence among state and local law enforcement agencies and various federal entities.

These fusion centers have been effective at sharing data across organizations within their own jurisdictions. Furthermore, their organizational structure makes it convenient for bilateral communication with federal entities and also allows the information to be further disbursed to other local entities when appropriate. Because peer fusion centers may contain law enforcement and disaster information relevant to one another but not of interest to the federal government, which is primarily interested in terrorist activity information, a mechanism for sharing this information would be valuable.

To meet this need, the Multistate Sharing Initiative (MSSI) was established in 2009 through Southeast Region Research Initiative (SERRI) sponsorship to assist these regional fusion centers with sharing information relating to a wider variety of state interests than just terrorism. To develop MSSI, Oak Ridge National Laboratory (ORNL) teamed with Cadre5, which is a private software development company, and with Southern Shield, which is a regional intelligence fusion center working group that includes all of the states in the southeastern region of the United States. ORNL, Cadre5, and Southern Shield determined that the first useful information to share through the MSSI would be Suspicious Activity Reports (SARs).

SARs are of special interest to multiple jurisdictions because the information contained, either specific or fuzzy, can influence multiple related law enforcement investigations where the direct impact of the SAR information is initially unknown to all consumers. This sharing of information can result in a better overall situational understanding by a consumer in another jurisdiction. For example, a statement indicating persons observing power plants, an out of place vehicle, or multiple people acting secretively and exchanging money would get recorded by a SAR stored in a local SAR repository. Other states may have similar reports in their own SAR repositories, but a better understanding of what may be occurring regionally could be obtained if an analyst had access to SARs in adjacent jurisdictions, even across state boundaries.

2. GOALS AND ISSUES

The goal of MSSI is to create a mechanism for interstate sharing of SAR data. Although other SAR sharing techniques are being developed and deployed by federal entities, their only goal is to share data with a nexus to terrorism. Very early in the development of state and local intelligence fusion centers it became clear that a mechanism to share SAR information relating to law enforcement and disaster issues in addition to terrorism-related information would be helpful to state and local jurisdictions. For example, suspicious activity related to drug trafficking cannot be shared using federally developed systems. MSSI would bridge this gap.

Development of the MSSI system presented several challenges. Simply creating an Internet based mechanism to share data was insufficient. Also, while it would be relatively easy to design a system to collect SAR information and install that information in multiple jurisdictions, many of the Southern Shield states already have a large investment in records management systems. Furthermore, their SAR data are already being collected and managed by their systems, and their users are already trained in and comfortable with using these systems. Therefore, developers realized that to be successful, MSSI would need to take advantage of and use these existing systems.

Additionally, the developers of the MSSI system had to address the issues of (1) system maintenance and management, (2) data ownership, and (3) security. Because the MSSI system would be deployed over several states, maintenance and management of the system would have to be achieved in such a manner as to be acceptable by all states involved. It was decided that the MSSI system would be decentralized so that each state would be responsible for managing and maintaining its portion of the system. If the system in any state was not maintained or managed and resultantly failed, then the systems in the other states would continue to operate. Ownership of the SAR data was handled in a similar manner. Each state maintained ownership of the data that were input to its portion of the system, and only the responsible or owner state could modify or change its information. Such information was shared with other states as read only copies to which they could add or append information. In regard to data security, because the MSSI system data and its transport network must be secure, each state is responsible for safeguarding its own information, and the transport network uses commonly accepted secure IPs.

3. STATE OPERATIONS

As will be seen in the following sections, some form of the MSSI SAR system is deployed in Alabama, Kentucky, Tennessee, and South Carolina. This section attempts to convey and document the experiences and insights of these states in using the system to exchange SARs. About 1 year after system implementation, cognizant fusion center personnel from each state were contacted to ascertain the status of their MSSI SAR systems. The state fusion center representatives contacted included the following.

- South Carolina:
  Intelligence Research Analyst Tim Frederick and Intelligence Research Analyst Spencer Packer
- Kentucky:
  Chief Information Officer of the Kentucky Office of Homeland Security Mary Pederson and Kentucky State Police Information Systems Manager Jerry Wright
- Tennessee:
  Fusion System Program Manager Tennessee Department of Safety Office of Homeland Security Malcolm Sloan and Codirector Tennessee Fusion Center Steve Hewett
- Alabama:
  Senior Project Manager Alabama Criminal Justice Information Center and Chairperson of the Southern Shield Technology Subcommittee Shane Hammett

The overwhelming response from these individuals was that the MSSI SAR system was an outstanding success and contributed greatly to the security and resiliency of their states. The states still operate their respective MSSI systems, which are currently being augmented by the federal government's Nationwide Suspicious Activity Reporting Initiative (NSI). One state representative commented that SERRI's implementation of the MSSI SAR system actually "jump started" and accelerated deployment and acceptance of the nationwide SAR system.

While all states were enthusiastic about their systems, South Carolina and Tennessee appeared to be the heaviest users of their respective systems. Tennessee uses both the MSSI SAR and the NSI systems and participates in the Federal Bureau of Investigation's eGuardian Program. With NSI taking the bulk of the load of sharing SARs with other states, Tennessee has redeployed the MSSI SAR system within Tennessee to allow SAR sharing between state and local organizations, including Tennessee's three Homeland Security Regions, 11Homeland Security Districts, and more than 500 police and sheriff offices and with other states. While Tennessee developed its version of the MSSI SAR system based upon Tennessee's Consolidated Records Management System, South

Carolina is operating the Economy SAR System or EconoSAR, which is described in detail later in this report. In one "success story" from South Carolina, EconoSAR was used to compile similar SARs from throughout the state, which were then forwarded to field liaison officers, emergency management personnel, and law enforcement officers for action. In another success story, SARs from EconoSAR were used as bullet points to defend analyses of specific threat scenarios.

Kentucky is currently in the process of implementing its NSI system and integrating it with its MSSI SAR system. Greater success is expected with the combined NSI-MSSI SAR system.

4. INFORMATION SHARING SOLUTION

Web services are a common technique used for sharing information between multiple systems over the Internet. Using a web service for information exchange in the MSSI system allows a defined communication scheme between states that is independent of the database structure containing the SAR information, which varies from state to state. Therefore, using a web service for information exchange for the MSSI system grants the ability to define a communication contract without detailing the underlying implementation. This hides the underlying databases storing SAR data and allows changes to the underlying SAR systems without breaking compatibility with the exchange mechanism.

To simplify creation of these web services, the Simple Object Access Protocol (SOAP) was used. Creating SOAP based web services has advantages across multiple development teams because SOAP is programming language agnostic and most programming languages and integrated development environments offer very simple tools for the creation of such services.

The web service for each state had to be identical from the perspective of any potential consumer (i.e., from state to state within the system). One mechanism to ensure this degree of consistency is a Web Services Description Language (WSDL) document. A WSDL document was created for MSSI to define the web service operations and the inputs and outputs of those operations. The MSSI WSDL document created by ORNL is shown in Appendix A.

The MSSI WSDL defines three operations: getMatches, getReportPDF, getReportAsNiemXML. The getMatches operation takes as input a list of keywords and returns a list of metadata about each SAR matching those keywords including an ID, number of matches per keyword, location, timestamp, and summary. This operation defines the basis of all searching that takes place in the system. Once a SAR has been identified and more details are needed, one of the other two operations can be used to retrieve details from the SAR. The getReportPDF operation takes a SAR ID as input and returns a Portable Document Format (PDF) representation of that SAR, and the getReportAsNiemXML operation takes a SAR ID as input and returns a document in a text format based on the Extensible Markup Language (XML) as defined by the National Information Exchange Model (NIEM) for SAR data.

The MSSI data ownership issue was also taken into consideration in the design of this WSDL. All operations defined by the WSDL are read only. There is no way for one state to modify data contained within another state's SARs. The getReport options for retrieving a specific SAR were defined to show a read only PDF format, and the XML structure is intended to be used by external systems as a read only technique as well.

The MSSI system began operation with the states of Alabama and Tennessee creating web services adhering to the ORNL defined WSDL. Each state had very different backend systems for managing SARs, but through the use of WSDL and web services, they were able to create identical mechanisms for retrieving SAR data.

While each state may implement its own software to consume this SAR information, the MSSI project team created a reference tool, called an "aggregator," to query each of these web services and aggregate the results into a single view. The aggregator was conceived as a web based search tool resembling the Google search interface in its simplicity.

Once a user enters keywords for a search (Fig. 1) and clicks the "Search SARs" button, the aggregator will connect to each state's web service in parallel and call the getMatches operation using the keywords. The results of all the calls are then combined and presented to the user in tabular form as shown in Fig. 2.

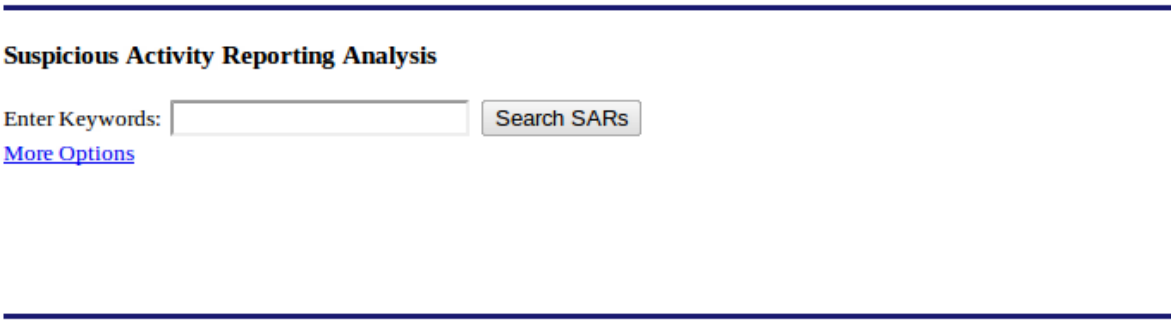

Fig. 1. SAR Aggregator search interface.

Suspicious Activity Reporting Analysis

Enter Keywords: arson Search SARs

More Options

State	Count
AL	24
KY	24
SC	24
TN	24

SAR ID	Rank	Keyword Match	Location	Timestamp	State
154	1	(total matches:2 - rank:2): keyword(arson:2)	Johnson City, Tennessee	11/21/2010 04:58:10 PM	SC
The colder the x-ray table, the more of your body is required stalking to be on it. The colder the x-ray table, the more of your body is required to explosives be on it. A lot of people are afraid arson of heights. Not me, I'm afraid of widths. The ...					
154	2	(total matches:2 - rank:2): keyword(arson:2)	Johnson City, Tennessee	11/21/2010 04:58:10 PM	AL
The colder the x-ray table, the more of your body is required stalking to be on it. The colder the x-ray table, the more of your body is required to explosives be on it. A lot of people are afraid arson of heights. Not me, I'm afraid of widths. The ...					
154	3	(total matches:2 - rank:2): keyword(arson:2)	Johnson City, Tennessee	11/21/2010 04:58:10 PM	TN
The colder the x-ray table, the more of your body is required stalking to be on it. The colder the x-ray table, the more of your body is required to explosives be on it. A lot of people are afraid arson of heights. Not me, I'm afraid of widths. The ...					
154	4	(total matches:2 - rank:2): keyword(arson:2)	Johnson City, Tennessee	11/21/2010 04:58:10 PM	KY
The colder the x-ray table, the more of your body is required stalking to be on it. The colder the x-ray table, the more of your body is required to explosives be on it. A lot of people are afraid arson of heights. Not me, I'm afraid of widths. The ...					
210	5	(total matches:2 - rank:1): keyword(arson:2)	Chattanooga, Tennessee	09/30/2010 04:58:11 PM	SC
The colder the x-ray table, the more of your body is required arson to be on it. The colder the x-ray table, the more of your body is required to arson be on it. A lot of people are afraid informant of heights. Not me, I'm afraid of widths. The seve...					
210	6	(total matches:2 - rank:1): keyword(arson:2)	Chattanooga, Tennessee	09/30/2010 04:58:11 PM	AL
The colder the x-ray table, the more of your body is required arson to be on it. The colder the x-ray table, the more of your body is required to arson be on it. A lot of people are afraid informant of heights. Not me, I'm afraid of widths. The seve...					
210	7	(total matches:2 - rank:1): keyword(arson:2)	Chattanooga, Tennessee	09/30/2010 04:58:11 PM	TN
The colder the x-ray table, the more of your body is required arson to be on it. The colder the x-ray table, the more of your body is required to arson be on it. A lot of people are afraid informant of heights. Not me, I'm afraid of widths. The seve...					

Fig. 2. SAR Aggregator search results.

Figure 2 shows the actual search summary for all states queried. This small table shows how many results were returned from each state and would show an error message for a given state if the state was unresponsive to the search request. The search results table shows the SAR ID from the state, the number of keyword matches per document, the location of the event, the timestamp of the event, the state returning the data, and a short summary of the SAR. The SAR ID column presents a hyperlink. When clicked, this link will call the getReportPDF operation from the originating state and present a PDF document of the SAR to the user.

Because SERRI sponsorship of MSSI was time limited and no continuing funding was available, it was not possible to create a centralized version of the aggregator. Therefore to allow each state to be in control of the system it would be regularly using, an independent aggregator is hosted by each state (Fig. 3). The aggregator is implemented as a Java based web application which runs on the open source Oracle Glassfish Application Server. This method provides the states a license free option to run the system with support options from Oracle.

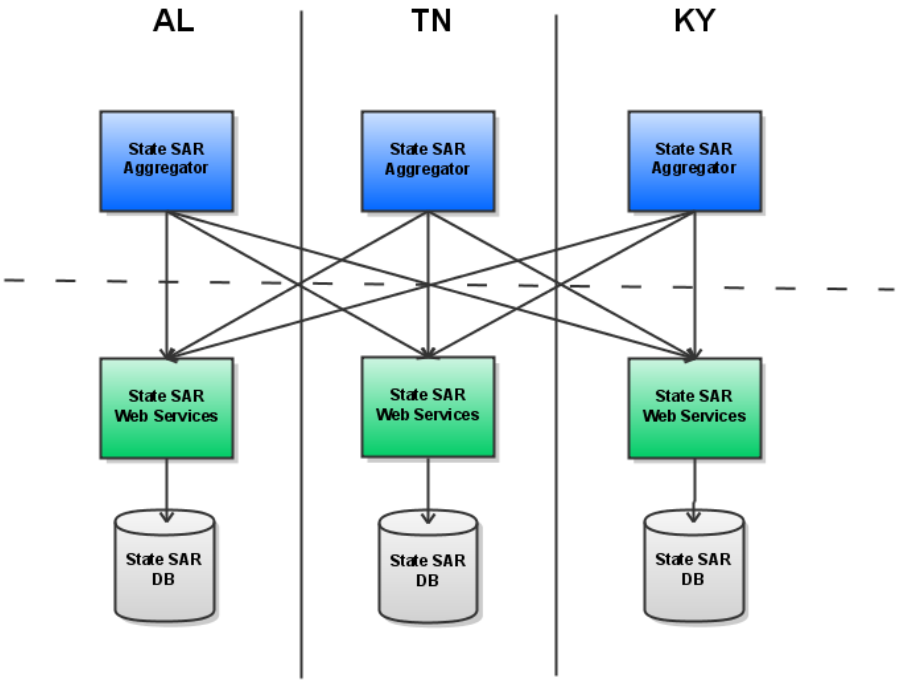

Fig. 3. SAR system deployment and communication model.

One security issue remained related to securing the information being exchanged. Some states embraced the low economic impact of using the public Internet, Secure Sockets Layer, and firewall rules, while other states criticized the technique as too insecure or burdensome on the network administrators to maintain the firewall rules for each entity. A private network would have been ideal but too expensive. The states already pay to be a part of Nlets,* so ORNL and Southern Shield convinced Nlets to host the traffic and even create a partitioned virtual private network for this endeavor at no additional cost to the states. Implementing this security improvement didn't require any change beyond issuing proper IP addresses and plugging the SAR server into the Nlets switch.

*Nlets is the International Justice and Public Safety Network, which links together and supports every state, local, and federal law enforcement, justice, and public safety agency for sharing and exchanging critical information.

5. KENTUCKY IMPLEMENTATION

Initial implementation of the MSSI system was in Tennessee and Alabama. Following successful implementation and several demonstrations, other states wanted to participate. Kentucky was identified as the next integration candidate because of its involvement with other related SERRI projects. While Kentucky wanted to participate and already had a state SAR database, at the time it did not have the resources to dedicate to developing the required MSSI web services. ORNL worked with Kentucky and developed these web services for the state.

The Kentucky State Police Information Technology organization provided a server in the Kentucky Intelligence Fusion Center to host the SAR Aggregator and SAR Web Services and established a virtual private network for the Kentucky MSSI network. ORNL installed the Oracle Glassfish Application Server and the SAR Aggregator software on this server and configured it to communicate with the Alabama and Tennessee systems. This allowed Kentucky to begin use of the MSSI SAR Aggregator while its web services were being developed.

ORNL was granted access to the Oracle database which stored the Kentucky SAR data. The first web service operation implemented was the getReportAsNiemXML operation. To create consistent, well formed XML, the FreeMarker template engine was used. This operation involved defining an object model to mimic the relevant parts of the Kentucky SAR relational model. Structured Query Language (SQL) queries were then defined using the popular MyBatis framework to populate the objects and enter into the FreeMarker template to generate clean, NIEM-compliant XML.

The next operation implemented was the getReportPDF operation. The queries and objects created for the getReportAsNiemXML were reused, but instead of passing the object structure into a FreeMarker template to generate XML, the objects were passed into a reporting template implemented using Jasper Reports. Jasper Reports was chosen over lighter weight Java based PDF generation application programming interfaces (APIs) because the PDF layout desired by Kentucky was very complex and Jasper provides a nice graphical drag and drop tool for creating reporting templates. This saved a considerable amount of development effort and resulted in very fast PDF generation.

The last and most difficult web service operation implemented was the getMatches operation. The basis of the getMatches operation is a keyword full text search. The Oracle database in Kentucky did not support the full text search extensions, and given the quantity of data in their database, the SQL "LIKE" operator using wildcards for keyword matching would have been prohibitively slow. Instead the Lucene API was used. A scheduled job was created that would run every 4 hours. This job would query all the SAR data from the database and rebuild a Lucene index. Subsequently, when keyword searches were issued to the system this Lucene based index would be used to retrieve a list of the relevant SARs and format the metadata appropriately for use by the getMatches web service operation.

With all three web service operations implemented, ORNL configured the Kentucky SAR Aggregator to query the Kentucky SAR data in addition to the Alabama and Tennessee data it was already retrieving. In addition, the Alabama and Tennessee SAR Aggregators were configured to use the Kentucky SAR web services.

6. ECONOMY SAR SYSTEM

Collection of SAR data by participating states is basic to MSSI. However, through discussions with multiple Southern Shield state fusion centers, MSSI developers determined that not all state fusion centers that wanted to participate in MSSI had a mechanism in place for managing and tracking SARs. As no SAR data were being electronically collected by these states, it would be impossible for them to fully participate. Therefore, the development team constructed a relatively

simple SAR recording system that any state that did not have an internal state SAR system would be able to install and use to participate. To make this system, called EconoSAR, as cost-efficient as possible for such states, it was based on freely available, open source software.

EconoSAR required a freely available, open source database to store the SAR information. While there are several very good, open source relational database products, MSSI chose the PostgreSQL database. PostgreSQL is known for being a very solid standards compliant database. PostgreSQL supports full text search, which is advantageous given the MSSI system searching needs. In addition, PostgreSQL has a spatial extension, called PostGIS, which could aid in implementing future enhanced features.

A web based user interface was required to avoid deployment issues. Because MSSI had already used the Oracle Glassfish application server for the SAR Aggregator, it was determined the user interface would be Java based and run in the Java Enterprise Edition compliant Glassfish container. The Spring Framework was chosen as a tool for structuring the user interface because it would provide excellent tooling for web model-view-controller framework, security for authentication and authorization, simple application configuration, and dependency injection. All of these features would allow the MSSI EconoSAR to have a robust, loosely coupled, modular software system.

EconoSAR Use Explanation

The first screen presented to users is a login screen (Fig. 4). No information is available without first logging in. The following roles are available to users at login.

- Viewer—can only search for and view SAR data
- Editor—can modify SAR data
- Auditor—can view history and audit trail for SAR data
- Admin—can configure system settings and manage users

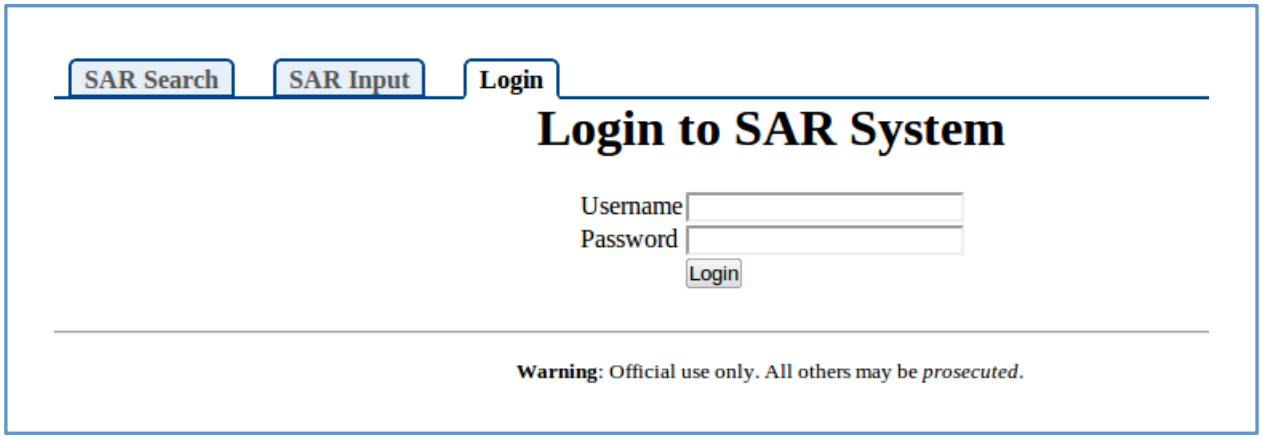

Fig. 4. EconoSAR login screen.

Once a user has logged in and been given appropriate privileges, the following actions are possible.

1. Search for SAR data (Figs. 5 and 6) [Viewer Role]—This function is similar to the search provided by the SAR Aggregator except that with this search the user can filter by more criteria than just keywords, and only the local database is being searched instead of cross-state searching.

Fig. 5. EconoSAR search form.

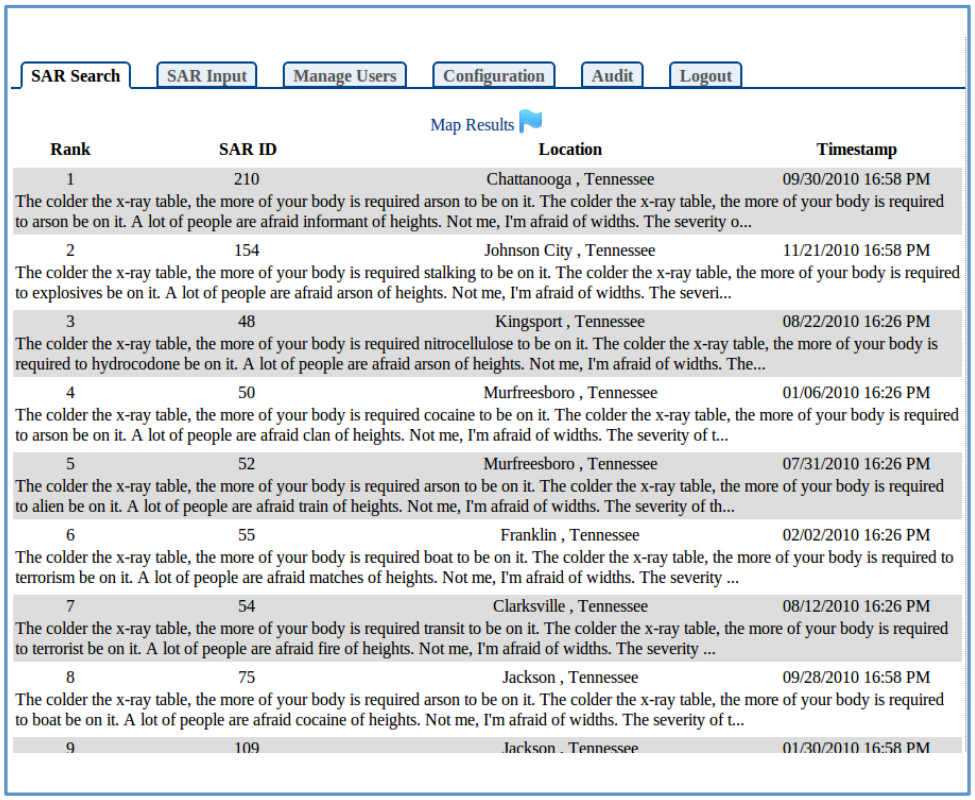

Fig. 6. EconoSAR search results.

2. Search and display by map [Viewer Role]—The Google Maps JavaScript API is used to present SAR data based on location in a map view (Fig. 7). Users can issue multiple searches which can then be refined, enabled, disabled, and overlain on top of other searches so an analyst can see whether there are correlations between various types of SARs and locations. Users may also choose to view the search results in Google Earth (Fig. 8).

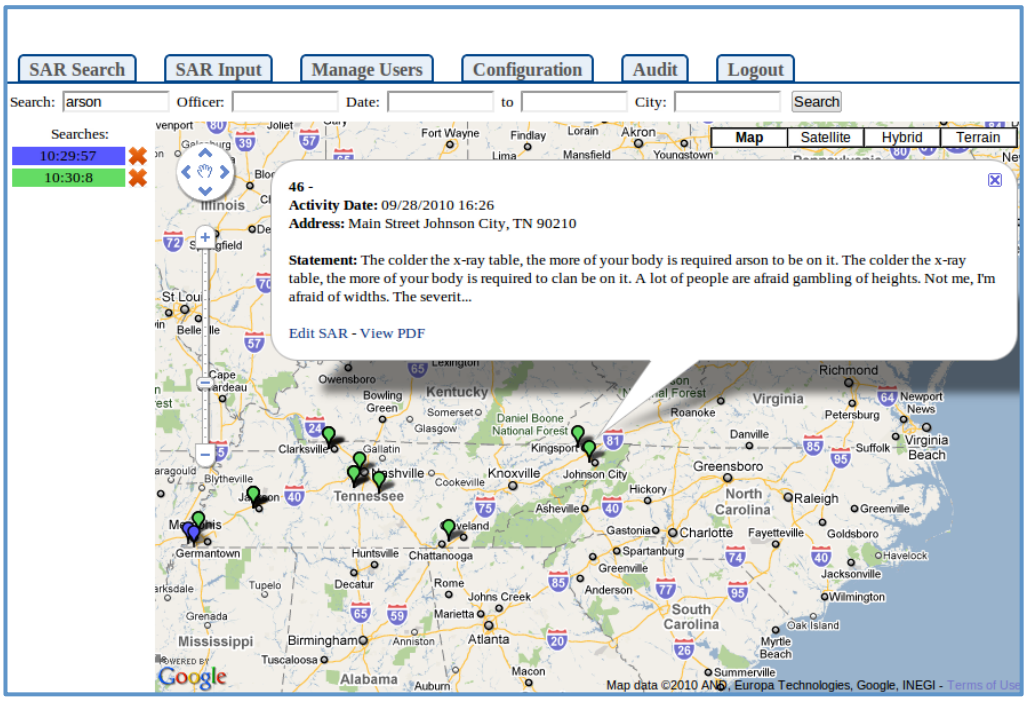

Fig. 7. EconoSAR map search interface.

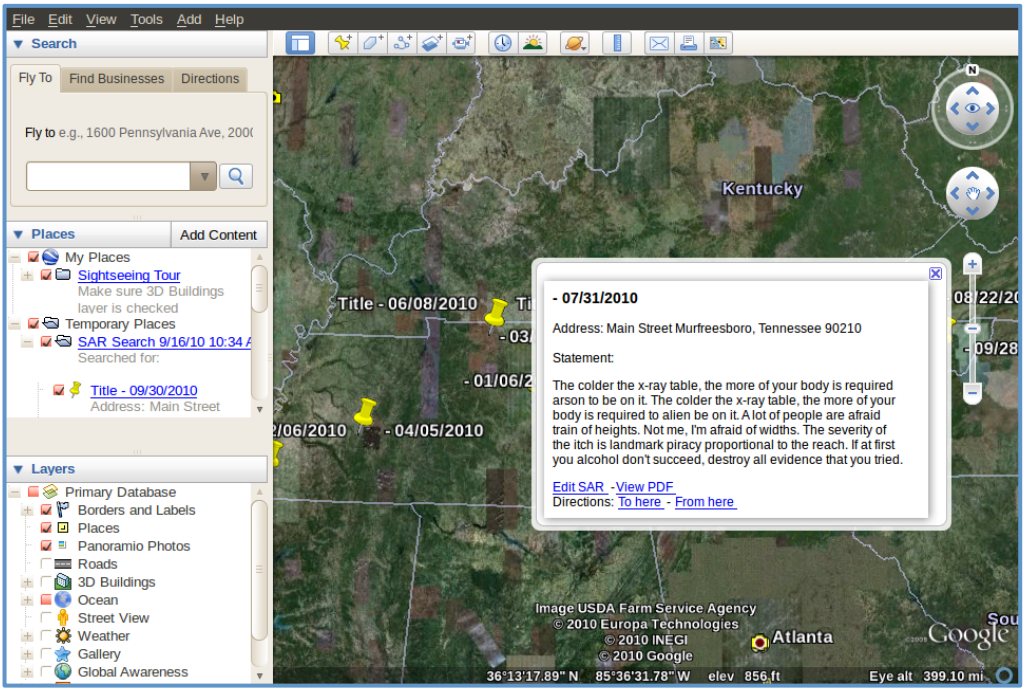

Fig. 8. EconoSAR search results in Google Earth.

3. Enter a new SAR (Figs. 9–14) [Editor Role]—Entering a SAR can be very complex. Because SARs document suspicious activity, the types and amounts of information they contain vary widely. Therefore, for any given SAR the amount of data entered in the system could be either extensive or quite sparse. Using the input tool, users can enter general SAR information such as date, time, and description (Fig. 9), but they can also enter additional information about law enforcement officers (Fig. 10), complainants (Fig. 11), subjects (Fig. 12), or vehicles (Fig. 13) involved in the suspicious activity. Users can also attach any available electronic files which may be related to the incident (Fig. 14).

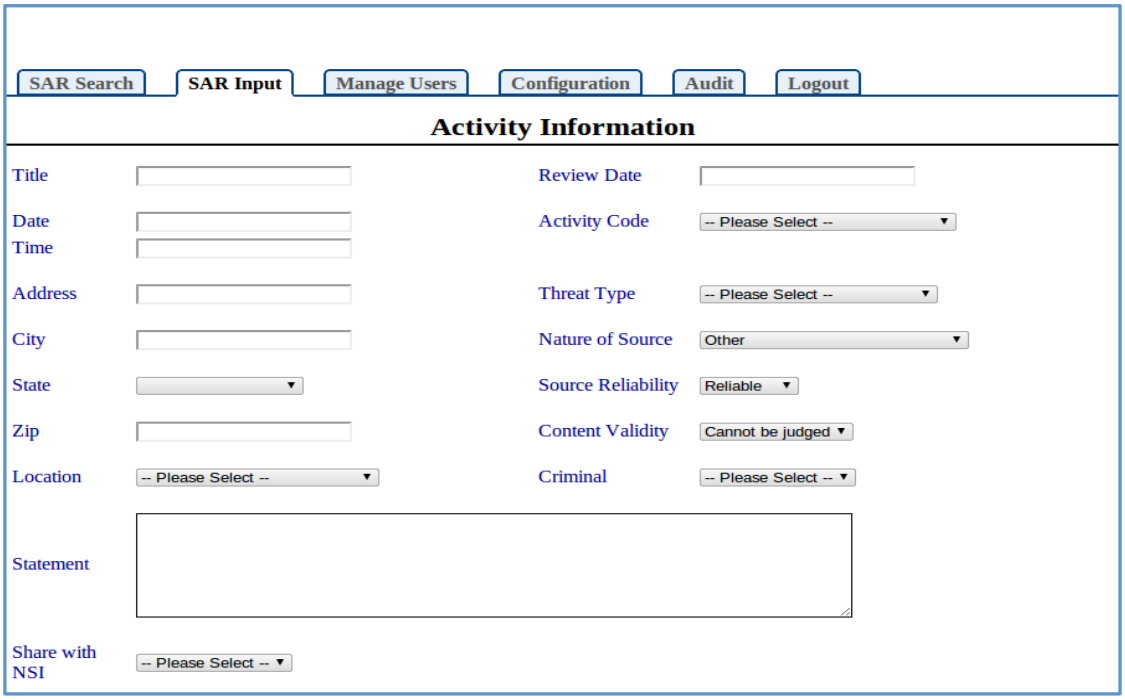

Fig. 9. EconoSAR activity information input screen.

Fig. 10. EconoSAR officer information input screen.

Fig. 11. EconoSAR complainant information input screen.

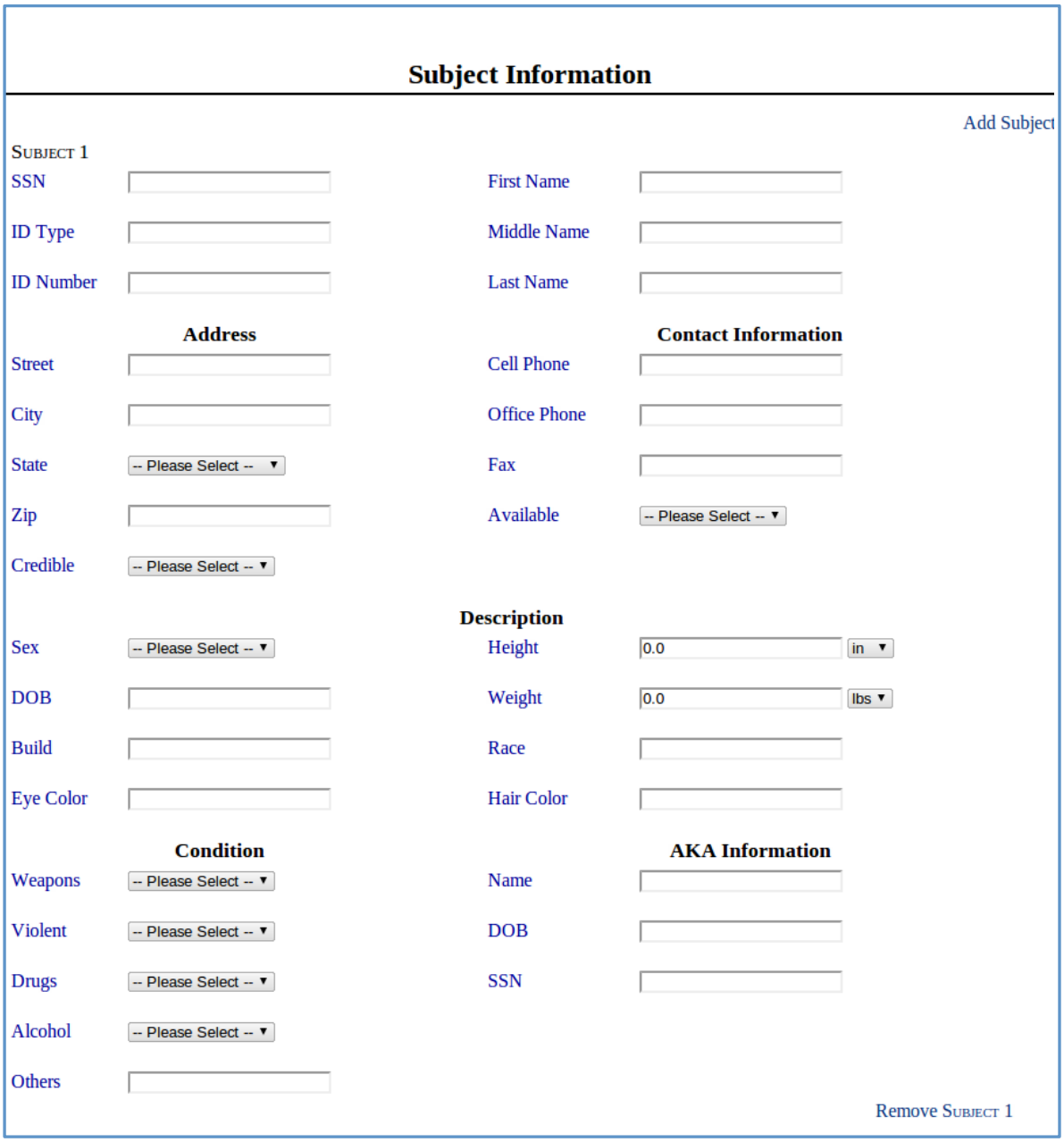

Fig. 12. EconoSAR subject information input screen.

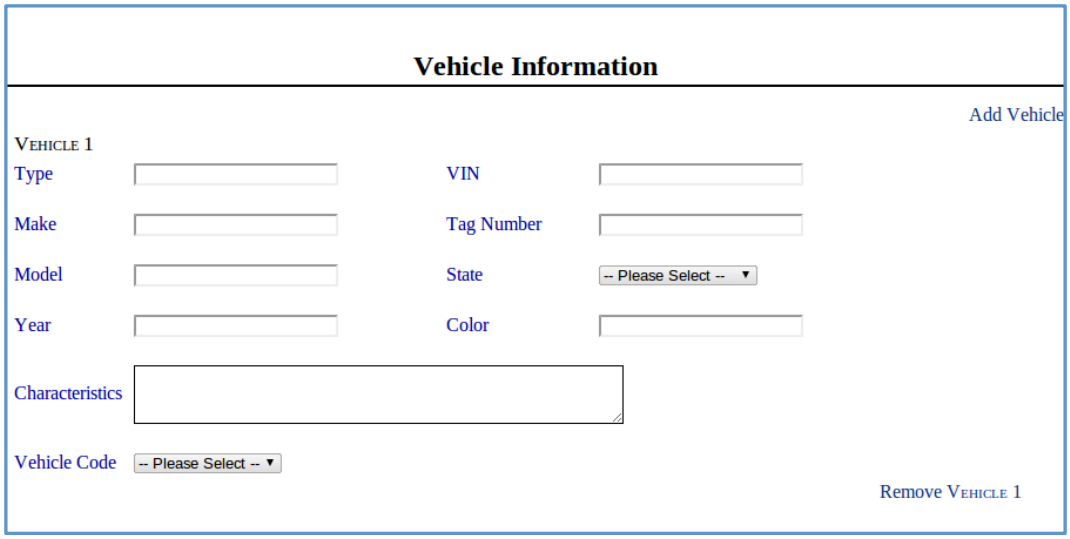

Fig. 13. EconoSAR vehicle information input screen.

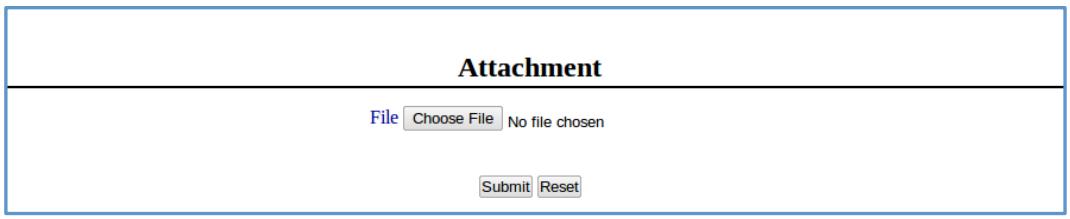

Fig. 14. EconoSAR attachments input screen.

4. Change an existing SAR [Editor Role/Auditor Role]

   (a) Editor Role. Once a user makes changes to a SAR, a historical copy of the original data is stored and an audit entry (Fig. 15) is created that identifies who changed the SAR and when the change was made.

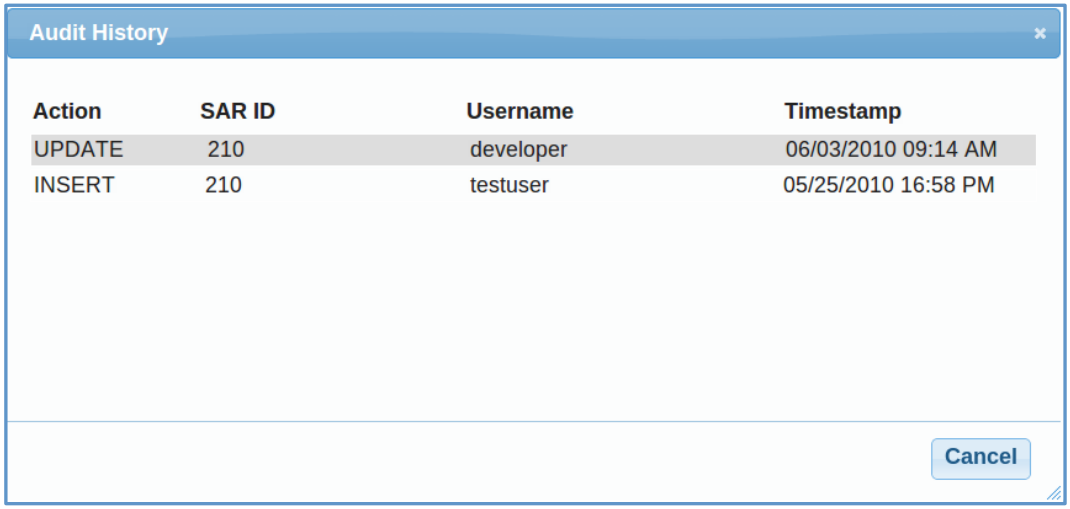

Fig. 15. EconoSAR audit history screen.

(b) Auditor Role. A user with auditor privileges will also be able to see the entire history of a SAR including when the SAR was modified and the responsible user. Users with auditor privileges may also search for the SARs a single user has changed or the SARs modified in a given time range (Fig. 16).

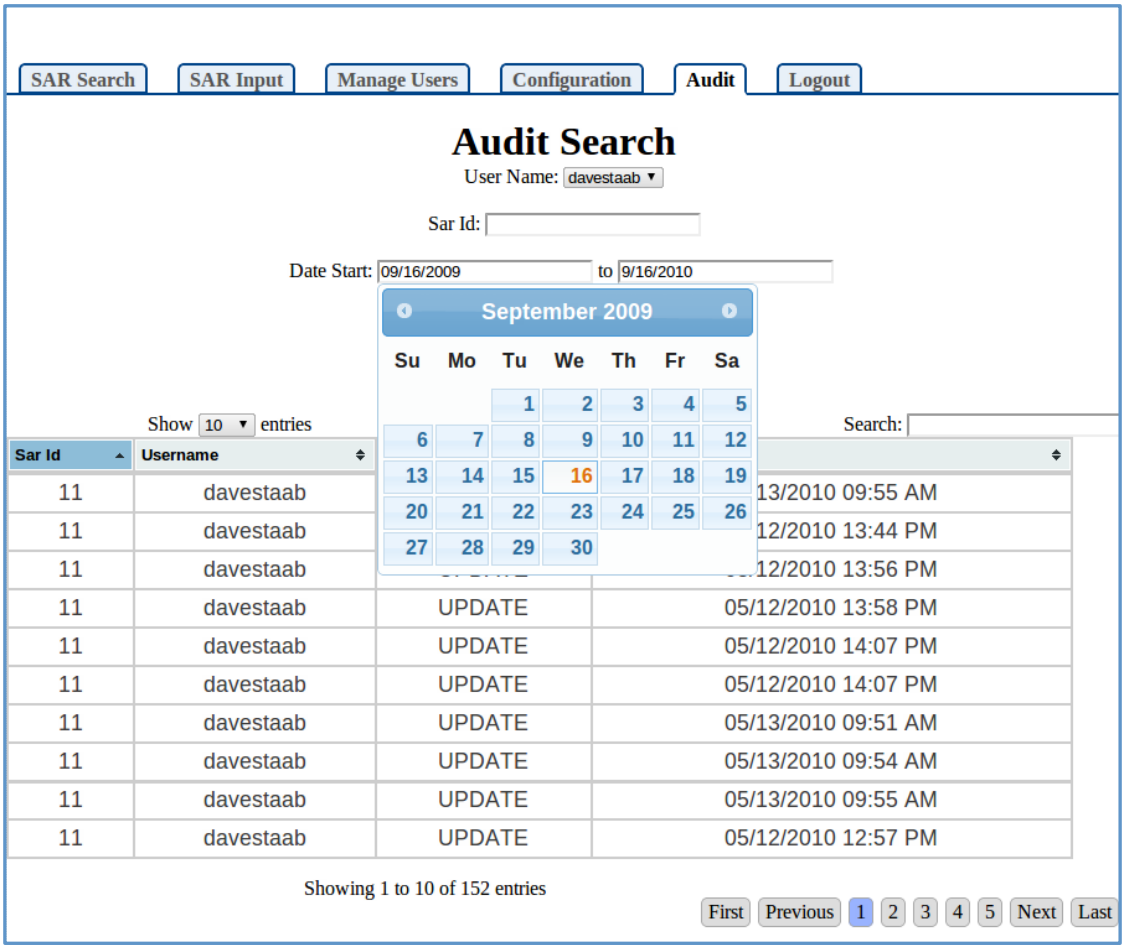

Fig. 16. EconoSAR audit search screen.

5. Create, disable, and manage users; change passwords; modify user roles (Fig. 17); and modify various other settings in the system (Fig. 18) [Admin Role], including the following:

   (a) the state in which the system resides,
   (b) settings for 28 CFR part 23 compliance,
   (c) legal footers at the bottom of each screen/page,
   (d) contact information,
   (e) communication settings for NSI,
   (f) email server settings (see also 6 below),
   (g) header images for the web site, and
   (h) header images for generated PDF documents.

   These options all exist to make this system flexible enough to work with the various operating procedures and local laws for any state that may need to use the system.

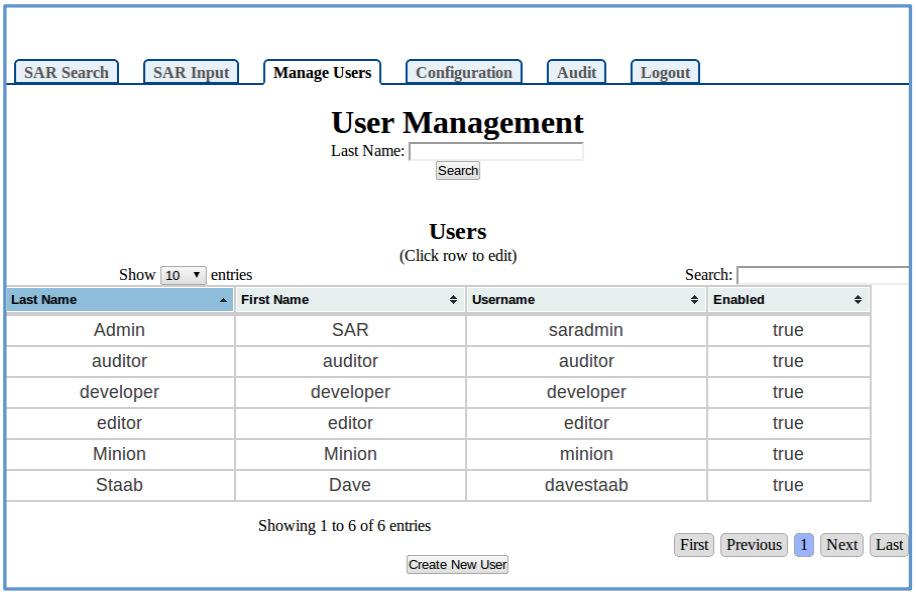

Fig. 17. EconoSAR user management screen.

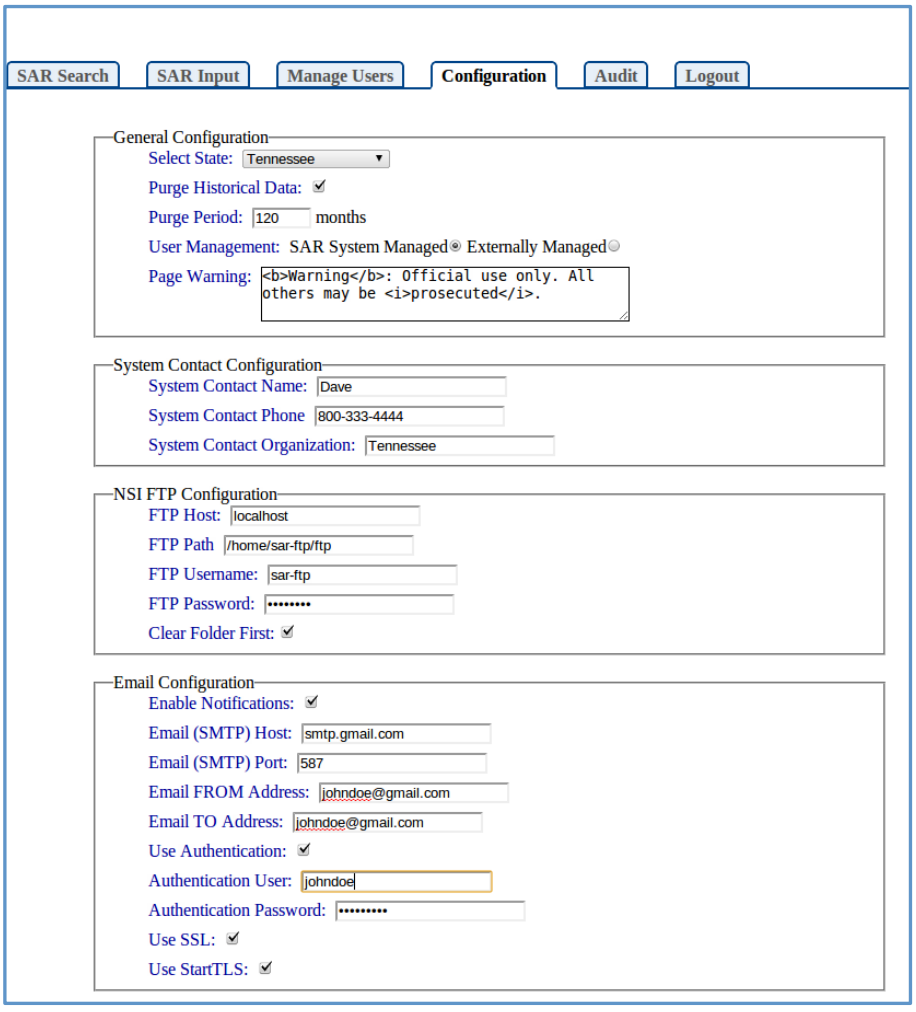

Fig. 18. EconoSAR administrative configuration screen.

6. Notify users when SARs are created or modified [Editor Role/Admin Role]—EconoSAR email settings can be configured [Admin Role] to access the email servers normally used by a state to send an email message indicating when a new SAR has been created or an existing SAR has been modified. This capability allows analysts to stay up-to-date on current suspicious activities without r manually searching the data each day.

7. SOUTH CAROLINA ECONOMY SAR IMPLEMENTATION

South Carolina was the first candidate for implementation of EconoSAR. The South Carolina Fusion Center was interested in participating in MSSI SAR sharing but did not have an electronic mechanism for storing and searching SAR data. As part of this project, therefore, ORNL provided technical assistance to the South Carolina Fusion Center and the South Carolina Law Enforcement Division to enable them to obtain a server and to install EconoSAR and the SAR Aggregator for use by South Carolina's intelligence analysts.

8. NATIONWIDE SUSPICIOUS ACTIVITY REPORTING INITIATIVE

Many of the states participating in the MSSI SAR sharing effort are also interested in participating in NSI. South Carolina is one of those states.

NSI is an outgrowth of a number of separate but related activities over the last several years that respond directly to the mandate to establish a "unified process for reporting, tracking, and accessing [SARs]" in a manner that rigorously protects the privacy and civil liberties of Americans as called for in the *National Strategy for Information Sharing*. The NSI strategy is to develop, evaluate, and implement common processes and policies for gathering, documenting, processing, analyzing, and sharing information about terrorism related suspicious activities. The long-term goal is for state, local, tribal, and federal law enforcement organizations and private sector entities to participate in NSI, allowing them to share information about suspicious activities that are potentially terrorism related.

The development team determined that EconoSAR would have to be expanded to bridge the gap between the MSSI and NSI systems, including building the ability to integrate with the NSI system into the EconoSAR software, to allow South Carolina to participate in NSI. In addition to facilitating South Carolina's participation in NSI, this would provide a much easier path for other states to begin participating in both MSSI and NSI because a solution would already exist for them to participate in both initiatives and the NSI team would already be familiar with how the software worked and comfortable with its reliability.

After much collaboration with the NSI team, the MSSI team expanded EconoSAR to successfully interoperate with the NSI Shared Space. The first NSI requirement was to give a user the ability to flag a SAR as being shareable with NSI. This field was added to the EconoSAR entry and edit forms. NSI also required several other fields to indicate the various types of activities, threat levels, and validity and reliability of each SAR. Each of these NSI-required fields were also added to the EconoSAR user interface, database, and XML data outputs.

Finally, a mechanism was needed to transfer the now compatible data to the NSI Shared Space. A data export module inside EconoSAR runs automatically on a scheduled basis to perform this function. This module queries the database for all SAR records flagged as shareable with NSI. It then creates NIEM-compliant XML documents for each SAR and FTPs them to a configurable location for the NSI system to consume.

9. CONCLUSION

The MSSI SAR effort has provided Southern Shield states a powerful toolset for sharing SAR information. Even states without an existing mechanism for SAR collection and management can now have a freely available software system with only the cost of the physical server to overcome.

The four pilot states of Alabama, Kentucky, South Carolina, and Tennessee are currently in production mode with the system, and additional states, including Louisiana and Arkansas, are currently investigating how to participate. In addition, Southern Shield is involved in ongoing discussions on how to grow the SAR Aggregator and web services to provide broader searching capabilities.

This effort has proven very useful to the state fusion centers and law enforcement agencies involved. We sincerely hope that this effort will continue to grow as more states become involved, enhancing the value to all participants.

10. REFERENCES

1. *Criminal Intelligence Systems Operating Policies (28 CFR Part 23)*; http://www.iir.com/28cfr/a.

2. *FreeMarker Java Template Engine Library*; http://freemarker.sourceforge.net/.

3. *Glassfish Application Server;* http://www.glassfish.org.

4. *JasperReports Java Reporting Library*; http://freemarker.sourceforge.net/.

5. *Lucene Indexing API*; http://lucene.apache.org/java/docs/index.html.

6. *MyBatis SQL Mapping Framework*; http://www.mybatis.org/.

7. *National Information Exchange Model*; http://www.niem.gov.

8. *National Strategy for Information Sharing; Successes and Challenges in Improving Terrorism-Related Information Sharing,* October 2007, http://www.fas.org/sgp/library/infoshare.pdf.

9. *National SAR Initiative; http://nsi.ncirc.gov/.*

10. *Nlets*; http://www.nlets.org.

11. *PostGIS Spatial Extension for PostgreSQL Database*; http://postgis.refractions.net/.

12. *PostgreSQL Database*; http://www.postgresql.org/.

13. *Simple Object Access Protocol*, World Wide Web Consortium, Apr. 2007*;* http://www.w3.org/TR/soap.

14. *Spring Framework*; http://www.springsource.org/.

15. *Web Services Description Language*, World Wide Web Consortium, Mar. 2001; http://www.w3.org/TR/wsdl.

APPENDIX A. MULTISTATE SHARING INITIATIVE WEB SERVICES DESCRIPTION LANGUAGE

APPENDIX A. MULTISTATE SHARING INITIATIVE WEB SERVICES DESCRIPTION LANGUAGE

```
<?xml version="1.0" encoding="utf-8"?><wsdl:definitions
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
    xmlns:tns="http://sarservices/ns/"
    xmlns:s="http://www.w3.org/2001/XMLSchema"
    xmlns:soap12="http://schemas.xmlsoap.org/wsdl/soap12/"
    targetNamespace="http://sarservices/ns/"
    xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
 <wsdl:types>   <s:schema elementFormDefault="qualified"
targetNamespace="http://sarservices/ns/">

    <s:element name="getReportPDF">       <s:complexType>         <s:sequence>          <s:element
minOccurs="0" maxOccurs="1" name="reportGUID" type="s:string" />         </s:sequence>
</s:complexType>     </s:element>
    <s:element name="getReportPDFResponse">       <s:complexType>         <s:sequence>
<s:element minOccurs="0" maxOccurs="1" name="getReportPDFResult"
          type="s:base64Binary" />         </s:sequence>       </s:complexType>     </s:element>
    <s:element name="getReportAsNiemXML">       <s:complexType>         <s:sequence>
<s:element minOccurs="0" maxOccurs="1" name="reportId" type="s:string" />         </s:sequence>
</s:complexType>     </s:element>
    <s:element name="getReportAsNiemXMLResponse">       <s:complexType>         <s:sequence>
<s:element minOccurs="0" maxOccurs="1" name="getReportAsNiemXMLResult"
          type="s:string" />         </s:sequence>
     </s:complexType>     </s:element>
    <s:element name="getMatches">       <s:complexType>         <s:sequence>          <s:element
minOccurs="0" maxOccurs="1" name="keywords"
          type="tns:ArrayOfString" />         </s:sequence>       </s:complexType>     </s:element>
    <s:complexType name="ArrayOfString">       <s:sequence>         <s:element minOccurs="0"
maxOccurs="unbounded" name="string"
          nillable="true" type="s:string" />       </s:sequence>     </s:complexType>
    <s:element name="getMatchesResponse">       <s:complexType>         <s:sequence>
<s:element minOccurs="0" maxOccurs="1" name="getMatchesResult"
          type="tns:ArrayOfArrayOfString" />         </s:sequence>       </s:complexType>
</s:element>
    <s:complexType name="ArrayOfArrayOfString">       <s:sequence>         <s:element
minOccurs="0" maxOccurs="unbounded" name="ArrayOfString"
          nillable="true" type="tns:ArrayOfString" />       </s:sequence>     </s:complexType>
   </s:schema>  </wsdl:types>
 <wsdl:message name="getReportPDFSoapIn">   <wsdl:part name="parameters"
element="tns:getReportPDF" />  </wsdl:message>
 <wsdl:message name="getReportPDFSoapOut">   <wsdl:part name="parameters"
element="tns:getReportPDFResponse" />  </wsdl:message>  <wsdl:message
name="getReportAsNiemXMLSoapIn">   <wsdl:part name="parameters"
element="tns:getReportAsNiemXML" />  </wsdl:message>
 <wsdl:message name="getReportAsNiemXMLSoapOut">   <wsdl:part name="parameters"
element="tns:getReportAsNiemXMLResponse" />  </wsdl:message>
 <wsdl:message name="getMatchesSoapIn">   <wsdl:part name="parameters"
element="tns:getMatches" />  </wsdl:message>
```

```
  <wsdl:message name="getMatchesSoapOut">    <wsdl:part name="parameters"
element="tns:getMatchesResponse" />  </wsdl:message>
  <wsdl:portType name="SARServiceSoap">    <wsdl:operation name="getReportPDF">
<wsdl:input message="tns:getReportPDFSoapIn" />      <wsdl:output
message="tns:getReportPDFSoapOut" />    </wsdl:operation>
    <wsdl:operation name="getReportAsNiemXML">      <wsdl:input
message="tns:getReportAsNiemXMLSoapIn" />      <wsdl:output
message="tns:getReportAsNiemXMLSoapOut" />    </wsdl:operation>

    <wsdl:operation name="getMatches">      <wsdl:input message="tns:getMatchesSoapIn" />
<wsdl:output message="tns:getMatchesSoapOut" />    </wsdl:operation>  </wsdl:portType>
  <wsdl:binding name="SARServiceSoap" type="tns:SARServiceSoap">    <soap:binding
transport="http://schemas.xmlsoap.org/soap/http" />
    <wsdl:operation name="getReportPDF">      <soap:operation
soapAction="http://sarservices/ns/getReportPDF"
          style="document" />      <wsdl:input>        <soap:body use="literal" />      </wsdl:input>
<wsdl:output>        <soap:body use="literal" />      </wsdl:output>    </wsdl:operation>
    <wsdl:operation name="getReportAsNiemXML">      <soap:operation
soapAction="http://sarservices/ns/getReportAsNiemXML"
          style="document" />      <wsdl:input>        <soap:body use="literal" />      </wsdl:input>
<wsdl:output>        <soap:body use="literal" />      </wsdl:output>    </wsdl:operation>
    <wsdl:operation name="getMatches">      <soap:operation
soapAction="http://sarservices/ns/getMatches"
          style="document" />      <wsdl:input>        <soap:body use="literal" />      </wsdl:input>
<wsdl:output>        <soap:body use="literal" />      </wsdl:output>    </wsdl:operation>
  </wsdl:binding>
  <wsdl:binding name="SARServiceSoap12" type="tns:SARServiceSoap">    <soap12:binding
transport="http://schemas.xmlsoap.org/soap/http" />
    <wsdl:operation name="getReportPDF">      <soap12:operation
soapAction="http://sarservices/ns/getReportPDF"
          style="document" />      <wsdl:input>        <soap12:body use="literal" />      </wsdl:input>
<wsdl:output>        <soap12:body use="literal" />      </wsdl:output>    </wsdl:operation>
    <wsdl:operation name="getReportAsNiemXML">      <soap12:operation
soapAction="http://sarservices/ns/getReportAsNiemXML"
          style="document" />      <wsdl:input>        <soap12:body use="literal" />      </wsdl:input>
<wsdl:output>        <soap12:body use="literal" />      </wsdl:output>    </wsdl:operation>
    <wsdl:operation name="getMatches">      <soap12:operation
soapAction="http://sarservices/ns/getMatches"
          style="document" />      <wsdl:input>        <soap12:body use="literal" />      </wsdl:input>
<wsdl:output>        <soap12:body use="literal" />      </wsdl:output>    </wsdl:operation>
  </wsdl:binding>
  <wsdl:service name="SARService">
    <wsdl:port name="SARServiceSoap" binding="tns:SARServiceSoap">      <soap:address
location="http://localhost" />    </wsdl:port>
    <wsdl:port name="SARServiceSoap12" binding="tns:SARServiceSoap12">      <soap12:address
location="http://localhost" />    </wsdl:port>

  </wsdl:service>
</wsdl:definitions>
```

APPENDIX B. SAMPLE SAR GETMATCHES WEB SERVICE REQUEST

APPENDIX B. SAMPLE SAR GETMATCHES WEB SERVICE REQUEST

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
                  xmlns:ns="http://sarservices/ns/">
   <soapenv:Header/>
   <soapenv:Body>
      <ns:getMatches>
         <ns:keywords>
            <ns:string>cocaine</ns:string>
         </ns:keywords>
      </ns:getMatches>
   </soapenv:Body>
</soapenv:Envelope>
```

APPENDIX C. SAMPLE SAR GETMATCHES WEB SERVICE RESPONSE

APPENDIX C. SAMPLE SAR GETMATCHES WEB SERVICE RESPONSE


```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
           xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
           xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Body>
    <getMatchesResponse xmlns="http://sarservices/ns/">
      <getMatchesResult>
        <ArrayOfString>
          <string>bf15991e-241f-428f-a64d-002e97febce9</string>
          <string>(total matches:1 - rank:1): keyword(cocaine:1)</string>
          <string>Homewood, Alabama</string>
          <string>5/13/2008 12:00:00 AM</string>
          <string>All those who cocaine believe in psychokinesis raise my
                  hand. If everything seems to be going well, you have
                  obviously overlooked murder something. The early bird
                  gets the worm, but the second military base mouse
                  gets the cheese. The sooner you fa...</string>
          <string>AL</string>
        </ArrayOfString>
        <ArrayOfString>
          <string>9a526e90-8e33-46f2-b1da-0091c361b3ff</string>
          <string>(total matches:1 - rank:1): keyword(cocaine:1)</string>
          <string>Mount Hebron, Alabama</string>
          <string>12/12/2007 12:00:00 AM</string>
          <string>A lot of people are afraid of heights. Not Suspicious
                  Vehicle me, I'm afraid of widths. I couldn't repair
                  your brakes, so chemical plant I made your horn
                  louder. When everything is coming your way, you're
                  cocaine in the wrong lane.</string>
          <string>AL</string>
        </ArrayOfString>
        <ArrayOfString>
          <string>8eb81ed1-6d58-44eb-b206-00c871f0b918</string>
          <string>(total matches:1 - rank:1): keyword(cocaine:1)</string>
          <string>Pine Hill, Alabama</string>
          <string>10/6/2007 12:00:00 AM</string>
          <string>The colder the Illegal Immigration X-ray table, the more
                  of your body is required to be on it. The severity
                  cocaine of the itch is proportional to the reach.</string>
          <string>AL</string>
        </ArrayOfString>
      </getMatchesResult>
    </getMatchesResponse>
  </soap:Body>
</soap:Envelope>
```

Southeast Region Research Initiative
National Security Directorate
P.O. Box 6242
Oak Ridge National Laboratory
Oak Ridge, TN 37831-6252

www.serri.org