NSI Shared Spaces Technical Description

1 Introduction

Implementation of the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) began in 2008 as a series of pilot projects at several state and local fusion centers. A NSI Evaluation Environment was created to test both business processes and information sharing technology and data standards. After a 12 month evaluation, the U.S. Attorney General directed that a formal NSI Program Management Office (NSI-PMO) be established to implement the NSI at all 72 DHS recognized fusion centers in the United States and selected federal agencies. As of March 1, 2010, the NSI PMO has been established within BJA to manage the coordination and deployment of NSI capabilities over a 3 year period.

1.1 Purpose and Scope

This document is intended for IT management supporting fusion center organizations that need to understand the manner in which the ISE-Shared Space application has been developed. More detailed documentation will be provided to each site as the program moves forward. This document will also provide the technology personnel at each site the ability to understand the general components of the applications provided by the NSI-PMO.

2 System Overview

This section provides a high level overview of the ISE-Shared Space concept that is being implemented across the NSI sites.

As depicted in Figure 1, each NSI participant has their own local source that hosts SAR data.

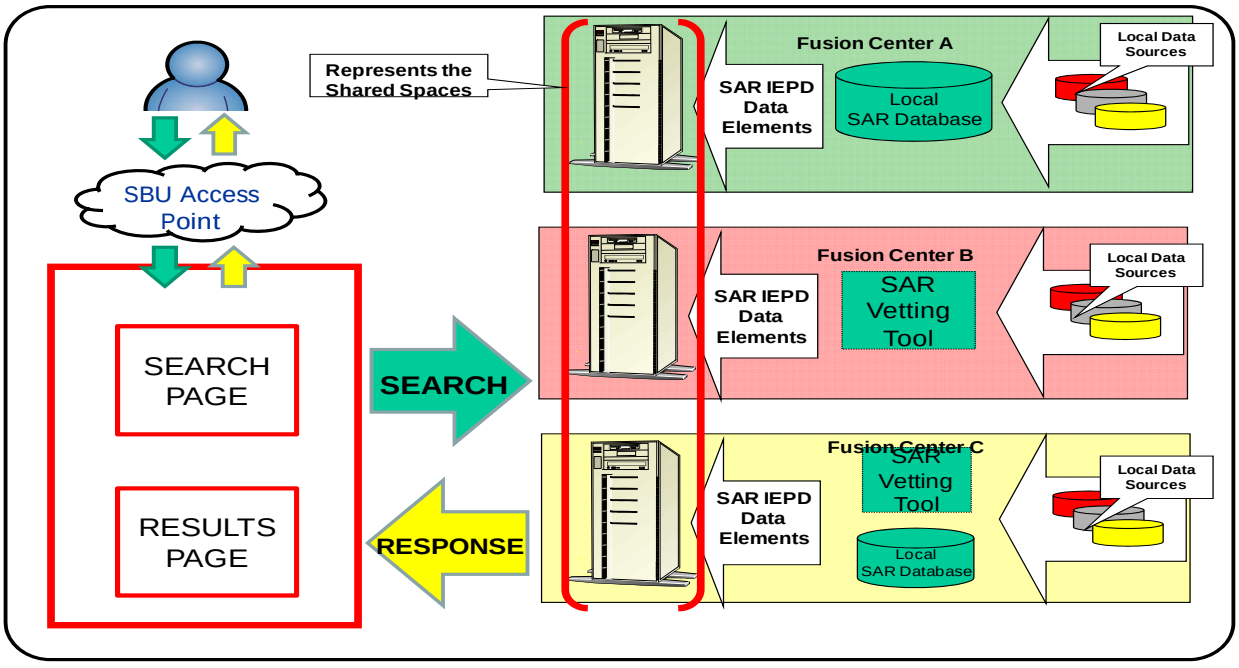

Figure 1, NSI Shared Space

Some of the local records management systems have the ability to support the vetting of SAR data in the source systems before forwarding it to the Shared Space. Other sites use a SAR Vetting Tool (SVT), developed by BJA at the request of several UASI fusion centers to enhance and vet SAR data to meet the Common Information Sharing Standards (CISS) and Information Sharing Environment (ISE) Functional Standards and Privacy guidelines. In both instances, those SARs that meet the criteria are then forwarded to the NSI Shared Space that resides locally at each NSI participant site as indicated by the servers contained within the red brackets. Any user from a NSI participant site that desires to search all the Shared Spaces will utilize the existing SBU networks (RISS, LEO and in the future, HSIN-Intel) to access the NSI Search Tool that resides at the secure National Criminal Intelligence Resource Center (NCIRC) portal (www.ncirc.gov).

As indicated in Figure 1 above, the Shared Space application comprises of two components. These are:

- Site Component
- Portal Component

The Site component consists of the software that resides at the local fusion center site or supporting data center. The Portal component consists of software that resides at NCIRC portal and is accessed by all the NSI users to conduct searches of the Shared Spaces.

Figure 2 depicts the manner in which all the Shared Spaces are accessed at this point.

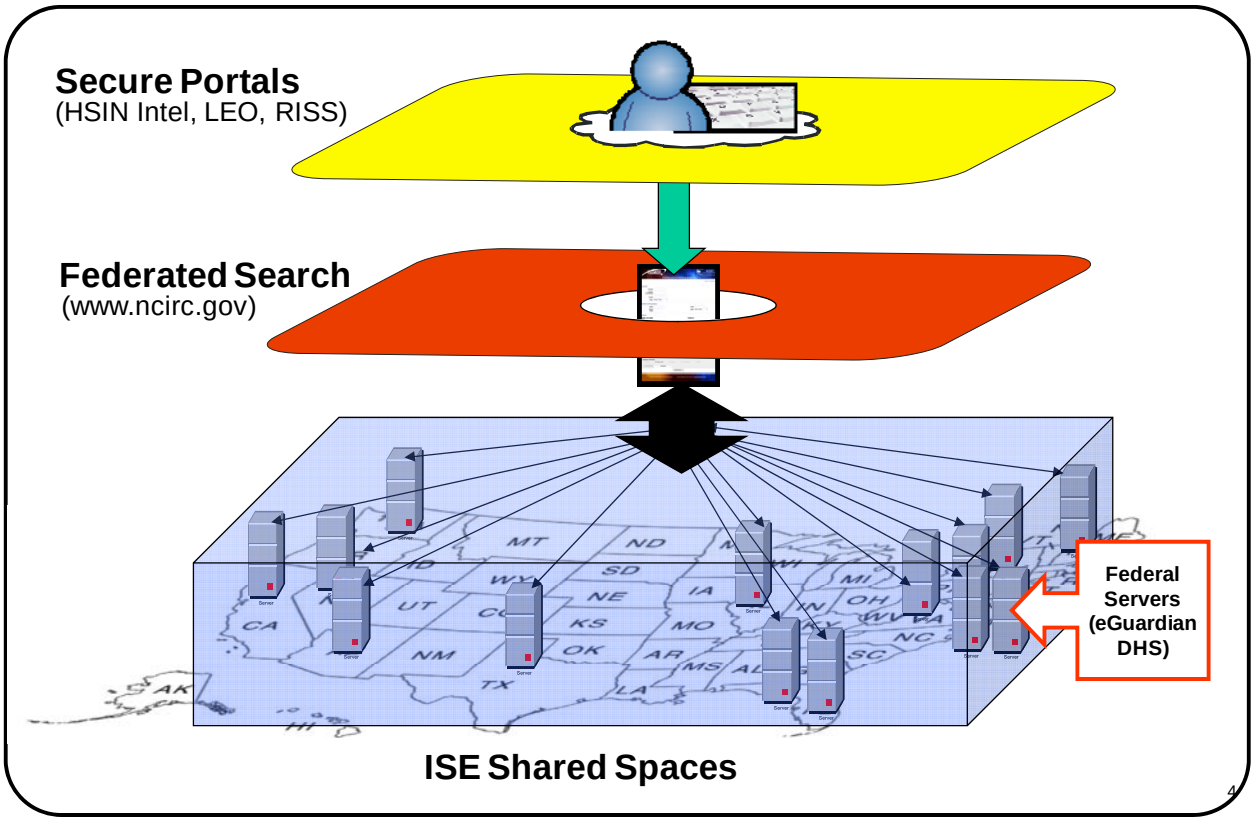

Figure 2, Shared Space

2.1 Document Organization

In order to assist the reader, this document is organized into multiple sections as described below:

Section 3: System Architecture. This section provides an understanding of the hardware and software architecture of the NSI Shared Space system.

Section 4: File and Database Design. This section discusses the manner in which the database has been designed for the NSI Shared Space application.

Section 5: User Interface. This section introduces a snapshot of the user interfaces designed for the NSI applications described in the previous sections.

2.2 Points of Contact

The ISE-Shared Space was developed under the oversight of the Bureau of Justice Assistance (BJA). For additional information on the ISE-Shared Space, please contact the following individuals:

David P. Lewis
Technical Manager, NSI PMO
Senior Policy Advisor
Bureau of Justice
US Department of Justice
810 7th Street, NW
Washington, DC 20531
David.P.Lewis@usdoj.gov
202-616-7829

Or:

Thomas O'Reilly
Director, NSI PMO
Senior Policy Advisor
Bureau of Justice Assistance
U.S. Department of Justice
810 7th Street, NW
Washington, DC 20531
thomas.o'reilly2@usdoj.gov
202-353-8590 (o)
202-598-5356 (c)

2.3 Glossary

SAR	Suspicious Activity Record
SVT	SAR Vetting Tool
ISE-SAR	Information Sharing Environment- Suspicious Activity Report
PM-ISE	Program Manager for the Information Sharing Environment
IEPD	Information Exchange Package Document
FBI	Federal Bureau of Investigation

SQL	Standard Query Language
WCF	Windows Communication Foundation
HTTP	Hyper Type Text Protocol
BJA	Bureau of Justice Assistance

3 System Architecture

This section describes the hardware and software architecture for the NSI Shared Space application. Figure 3 below represents a generic NSI architecture that includes all components available to the fusion centers.

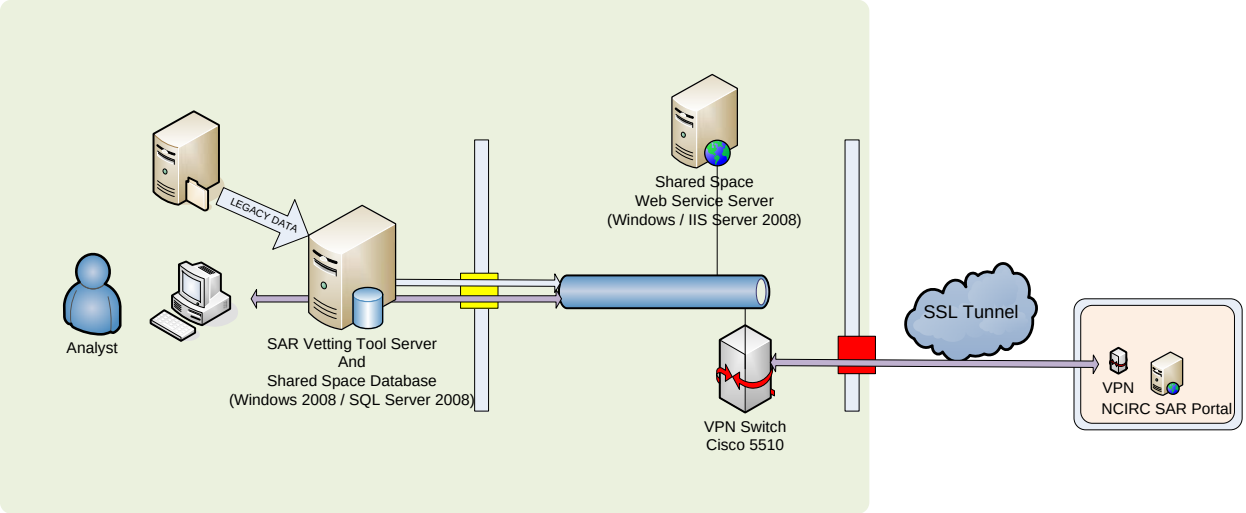

Figure 3 – Generic NSI Architecture

As shown, there are six primary components:

- Fusion Center Legacy system (s) used to process and hold SARs today.
- The SAR Vetting Tool software application and database
- The NSI Shared Space Database (usually co-located with SVT to share resources)
- NSI Shared Space Web Service Server
- Virtual Private Network Switch (Cisco 5510)
- NCIRC Portal and VPN connection

From a conceptual level (left side of diagram), an agency would use existing systems to initially capture and analyze SAR reports. If the legacy system did not conform to the ISE-SAR Functional Standard and coding conventions, then the agency could elect to push selected SARs to the SAR Vetting Tool application where Analyst's could enter required fields and improve the content and quality of the SAR data. Based upon Agency policy, SARs in the SVT would be pushed periodically to the NSI Shared Space database and then made available for searches by the NSI community. If the legacy system conforms to the Functional Standard, then the SVT application is not necessary.

The right side of the diagram illustrates the components involved in the NSI Search feature. Authorized users would log on to the NSI Search Tool hosted at the DOJ managed NCIRC.Gov portal. Users would then enter NSI search parameters into the web-based search page, selected NSI sites to search and issue a query. Using federated search technology, the search tool will issue separate search requests to web servers at the selected fusion centers via the installed VPN device. The Web server will forward the query request to the NSI Shared Space database at that fusion center. The query will be executed, results formatted as a LEXS based transaction, and returned to the web server for transmission back to the search tool at NCIRC. All results from multiple fusion centers retrieved in response to the query request will be aggregated, sorted and presented to user for analysis and action as appropriate. Note: an overview of the NSI search user interface is provided later in this appendix. Graphically, the search process is presented in Figure 4.

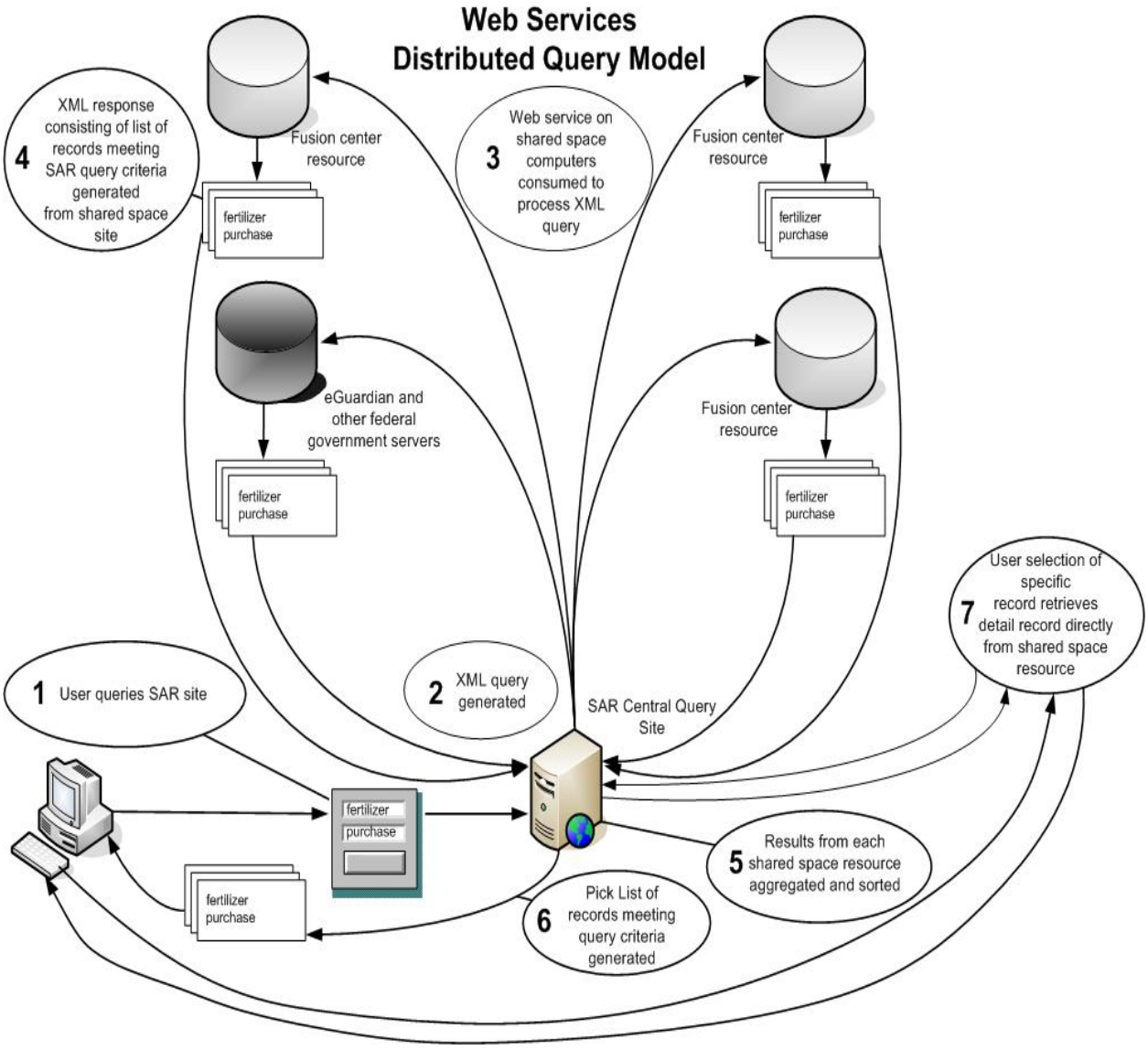

Figure 4. NSI Search Process

3.1 Hardware Architecture

As presented in Figure 5, the NSI Shared Space site component typically resides on one or two servers. It must be noted that there are two types of configurations that exist at the NSI participating sites. The first configuration is presented in 5. The second type of configuration is where only one server exists. While this document discusses the 2 server configuration, the primary difference is that in the 1 server configuration both the web server and the database server reside on the same server.

As depicted earlier in Figure 3, each site is connected to the NCIRC portal through a CISCO 5510 VPN router. This 5510 model was selected for its flexibility, connection features and ease of programming and installation although other standards VPN devices can be deployed. This router connects the ISE-Shared Space to the NCIRC portal providing for a secure, encrypted point to point interface. The connectivity between the NCIRC Portal and NSI Shared Space is accomplished via an encrypted IPsec VPN tunnel. The number and placement of firewalls is a local fusion center / IT data center decision.

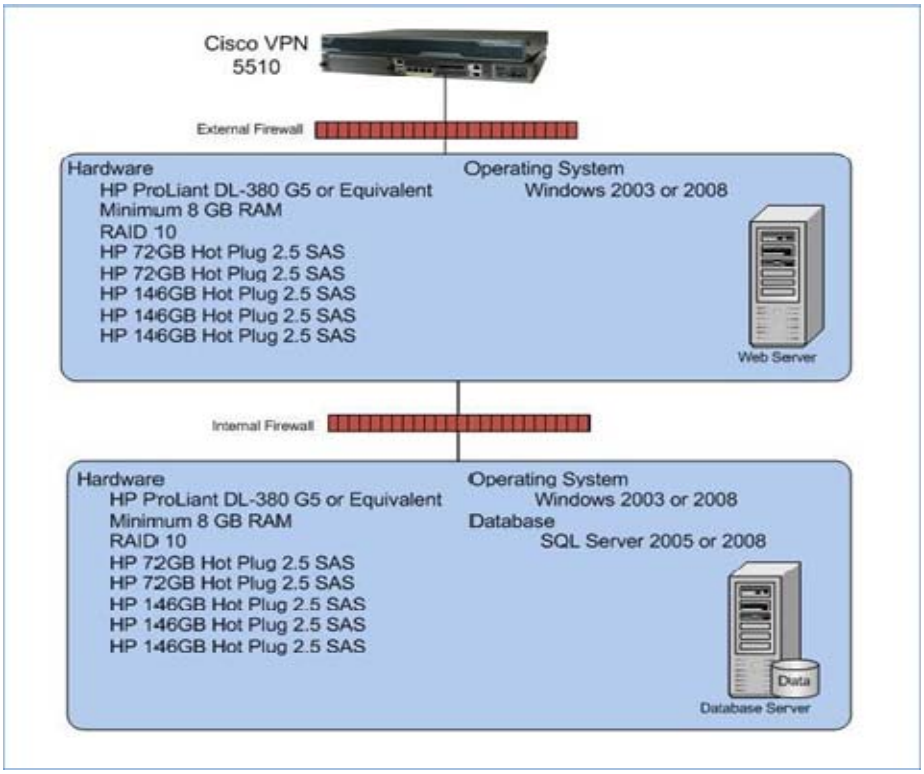

Figure 5, Technology Architecture

To date, most sites have selected either the HP ProLiant DL-380 servers or Dell PowerEdge servers. These models were selected because of their popularity at many of the fusion centers and their general purpose capabilities. The NCIRC Portal site uses Dell PowerEdge equipment. During the initial deployment of systems for the NSI Evaluation sites, only minimum server configurations were installed to minimize software licensing costs. In addition, no provision for failover or system redundancy was included. With the formal creation of the NSI, existing site configurations will be upgraded over time.

3.2 Software Architecture

The following table defines the latest versions of the software, including application software, installed within the typical NSI Shared Space Environment supporting the fusion center and on the NCIRC Portal.

Web Server:

Description	Configured Value
Shared Space	LEXS-SR 3.1.2
Operating System Version	Windows 2008 server
IIS Version	IIS 7.0
.NET Framework	.NET 2.0

Table 1: Web Server Software

Database and optional SVT Server:

Description	Configured Value
Operating System Version	Windows 2008 server
Database Version	SQL Server 2008
PERL Version	Active Perl 5.10

Table 2: Database Server and SAR Vetting Tool Software

NCIRC Portal Server:

Description	Configured Value
Operating System Version	Windows 2008 server
Database Version	SQL Server 2008
IIS Version	IIS 7.0
.NET Framework	.NET 3.5

Table 3: NCIRC Portal Server Software

3.2.1 NCIRC Portal Software:

Microsoft Windows 2008 is used for the operating system. This allows support of Microsoft Internet Information Services 7 as the web server supporting the application written in Microsoft's .NET 3.5. Microsoft SQL Server 2008 was utilized for database functions used by the SAR Portal application. Visual Studio 2008 Professional was used as the development tool for this application.

The NCIRC Portal application was developed in C# .NET due to familiarity with the software tools and language. The same decision applies for SQL, IIS and Windows Server.

The NCIRC Portal application was developed with two distinct components. The first is a presentation layer which provides the user interface. The second is the service layer which performs asynchronous queries to the multiple shared spaces. The presentation layer allows

users to search selected Fusion Centers which then passes the query to the service layer. The service layer then spreads the query to the selected Fusion Centers waiting for their response. Once the response is returned from the centers, the service layer collates the information and returns it to the presentation layer which then displays them for the user.

The user can then select a record to view the details on. The service layer then directly queries the fusion center to get the full record. This full record is displayed to the user for review.

3.2.2 Site Software Configuration:

The software architecture for the NSI Shared Space site component is presented graphically in Figure 6. This architecture can be viewed as having the following layers:

Service Interface Layer: The service interface layer has two primary responsibilities: Define and implement service contracts, and Implement service adapters.

Business Layer: The Business Layer contains components used to implement the business logic.

Resource Access Layer: The resource access layer is the layer between the business layer and the database. This layer implements the mechanisms for storing and retrieving data from the database.

Data Layer: This tier represents the database components that are utilized for the ISE-Shared Space. In some sites, MS SQL Server 2005 has been utilized and in other MS SQL Server 2008 is utilized.

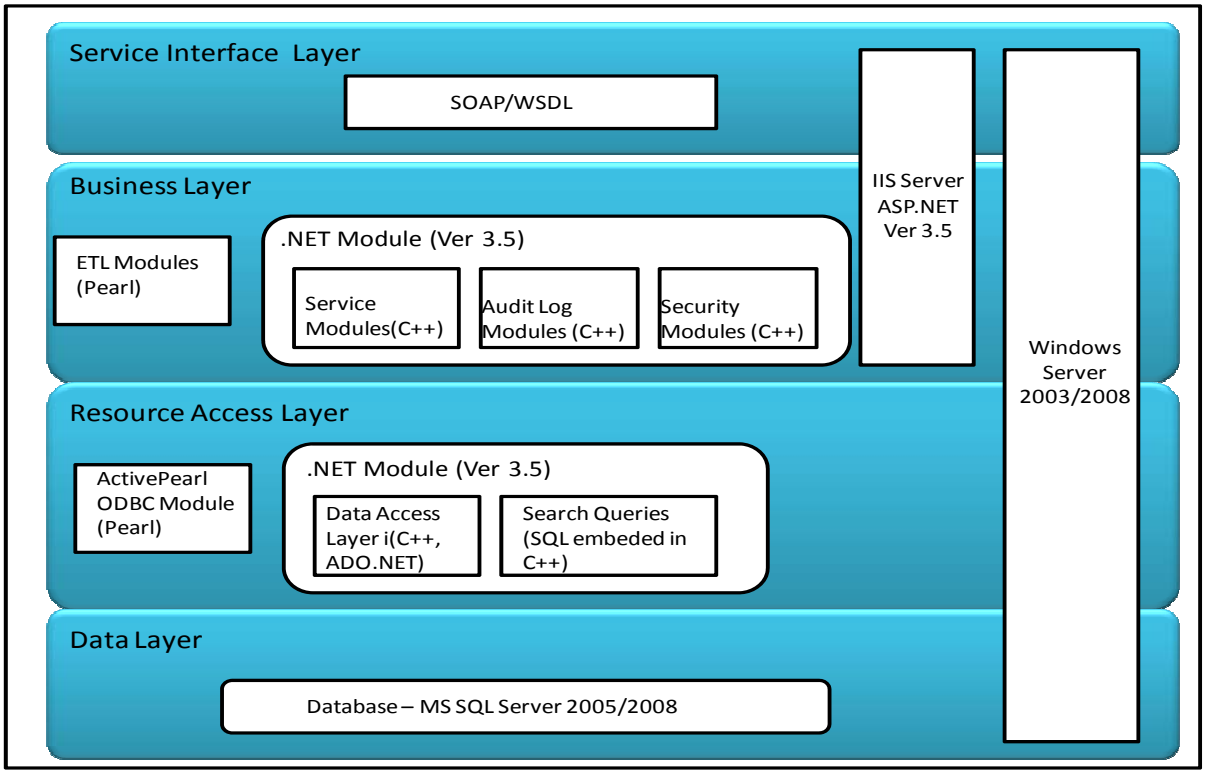

Figure 6, Application Architecture

These layers are discussed in greater detail below.

3.2.3 Service Interface Layer

The service interface layer for the application handles all the contracts and the service adapters for the NSI Shared Space service. It has the WSDL that describes the operations that the service will perform, the format of the information that is passed to and from the service and the message exchange pattern that is implemented. This is implemented using a SOAP message.

3.2.4 Business Layer

The Business Layer contains all the business logic for the service. The business layer has been implemented using the .NET, version 3.5 framework. This layer contains all the service logic modules, the audit log and the security modules. As described in Figure 6, this layer also encapsulates the ETL components that have been developed using ActivePearl software. The ETL module transforms the message from the legacy system and stores it in the data layer using the resource access layer described below.

3.2.5 Resource Access Layer

The resource access layer is responsible for persisting business entities to the data layer and retrieving individual business entities or sets of business entities on behalf of the business layer. The resource access layer for the ISE-Shared Space has been implemented using the .NET ver 3.5 framework and contains the Data Access layer and the Search queries. The resource access component of the ETL module also resides in this layer.

3.2.6 Data Layer

The data layer stores the SAR information for the specific location. This layer uses a Microsoft SQL Server database (either 2005 or 2008 versions). SQL Server was selected as a cost effective solution for fusion centers to maintain and consistent with the low operational loads anticipated with the NSI in general.

The Data Access Layer is the layer that supports the Business Access Layer to perform the actual search and retrieval functions on the database. The Data Access Layer is also responsible for converting the input request into a database SQL query and converting the results to an XML format that can then be returned to the client through the business access layer.

Note: the SVT application shares the MS SQL database but is essentially a separate application used to collect and vet SARs prior to the publishing of the data in the NSI Shared Space database.

4 File and Database Design

This section presents the database design that supports the NSI Shared Space application at each NSI site. The first part of this section presents the Entity Relationship (ER) diagram for the SAR Related component of the data model (Figure 3). Entity Relationship Diagram

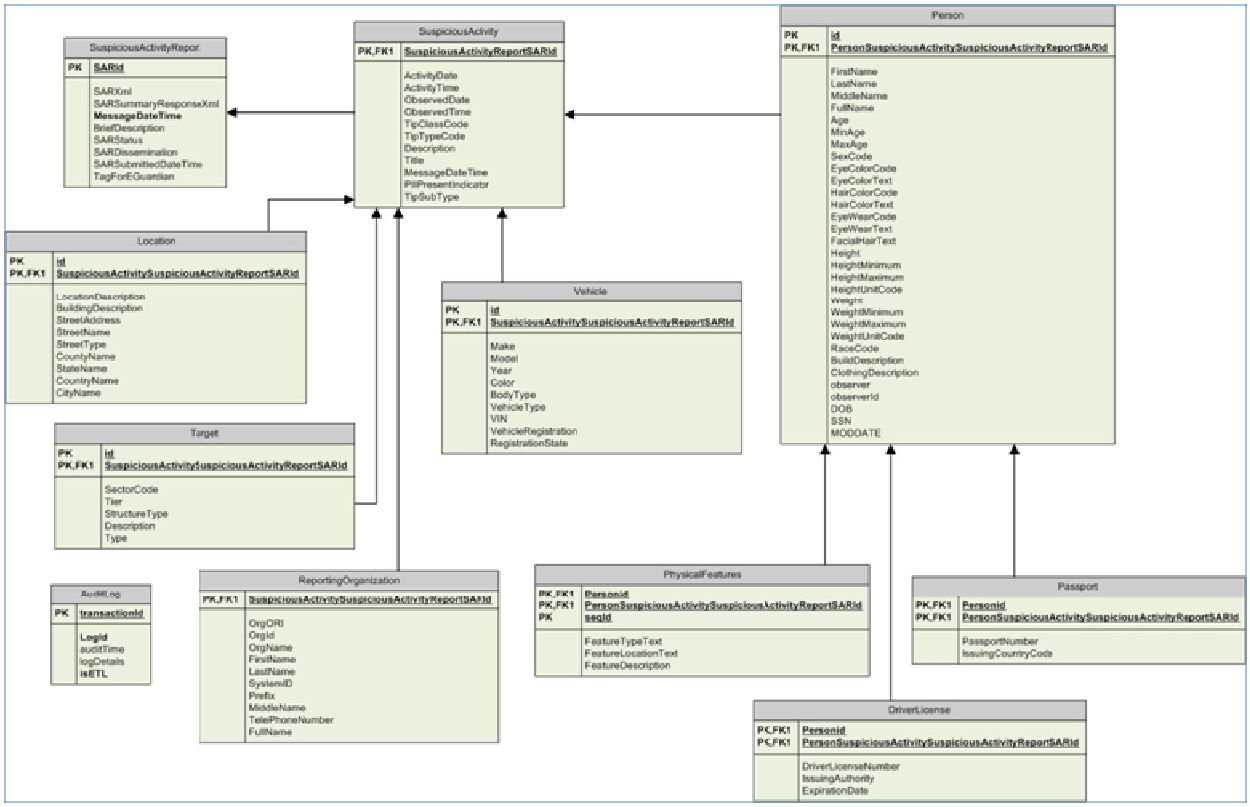

Figure 3, NSI Shared Space ER Diagram

5 User Interface

For the NSI project, DOJ elected to utilize the existing National Criminal Intelligence Resource Center portal to host the NSI Search Tool. User's that are authorized by participating NSI fusion centers and/or the NSI PMO with LEO or RISS accounts may access the portal and execute NSI searches. The figures contained in this section of Appendix C contain fictional data.

Figure 8 represents the standard NSI query screen used to enter search parameters (format as of March 2010). While some minimum fields are required, the user is free to query on any number of fields as well as conduct free text searches. In addition, the user has the option to select specific fusion centers to search.

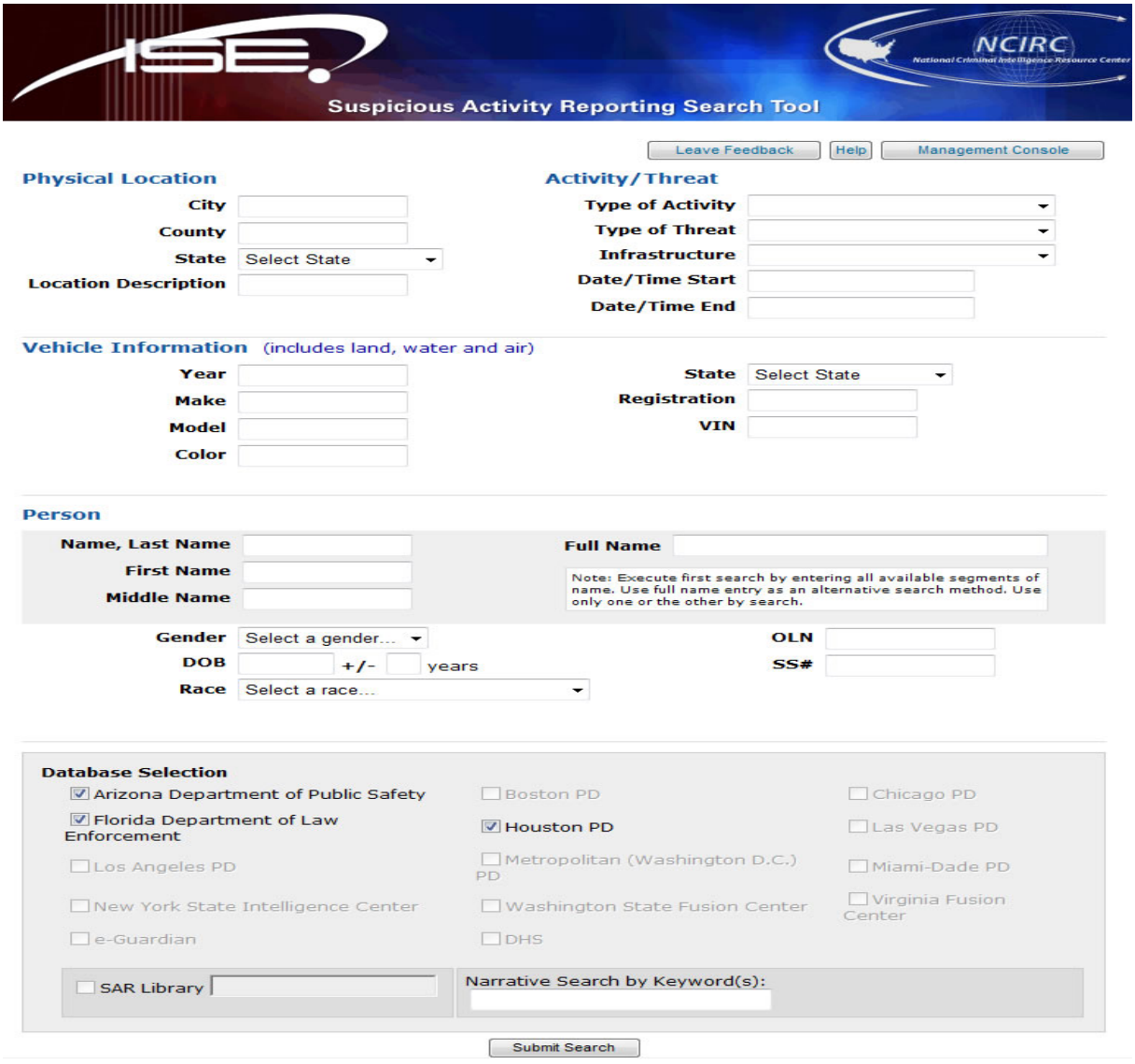

Figure 8. NSI Search Tool Query Request Screen

Figure 9, represents a typical summary results page that would be retrieved based on a search. In this case a search was conducted against the Houston (HRIS) fusion center and ten records were retrieved (two shown on the screen shot).

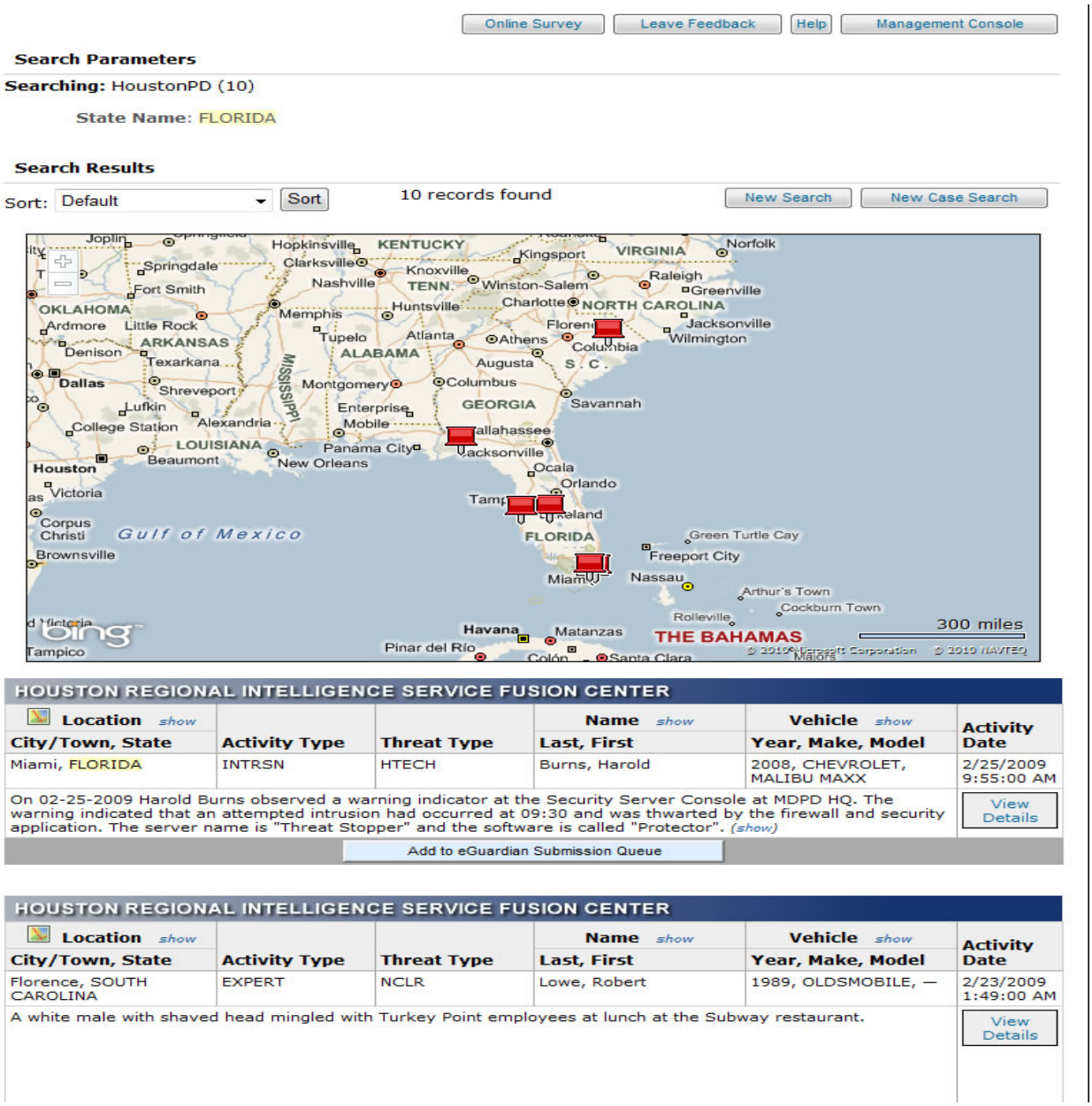

Figure 9. NSI Search Tool Summary Results Screen

The user has the option to see detailed data on a specific record, to include attachments if any, by clicking the “View Details” button on the left of the screen.

Figure 10 represents the detailed SAR report for a selected SAR from the previous screen.

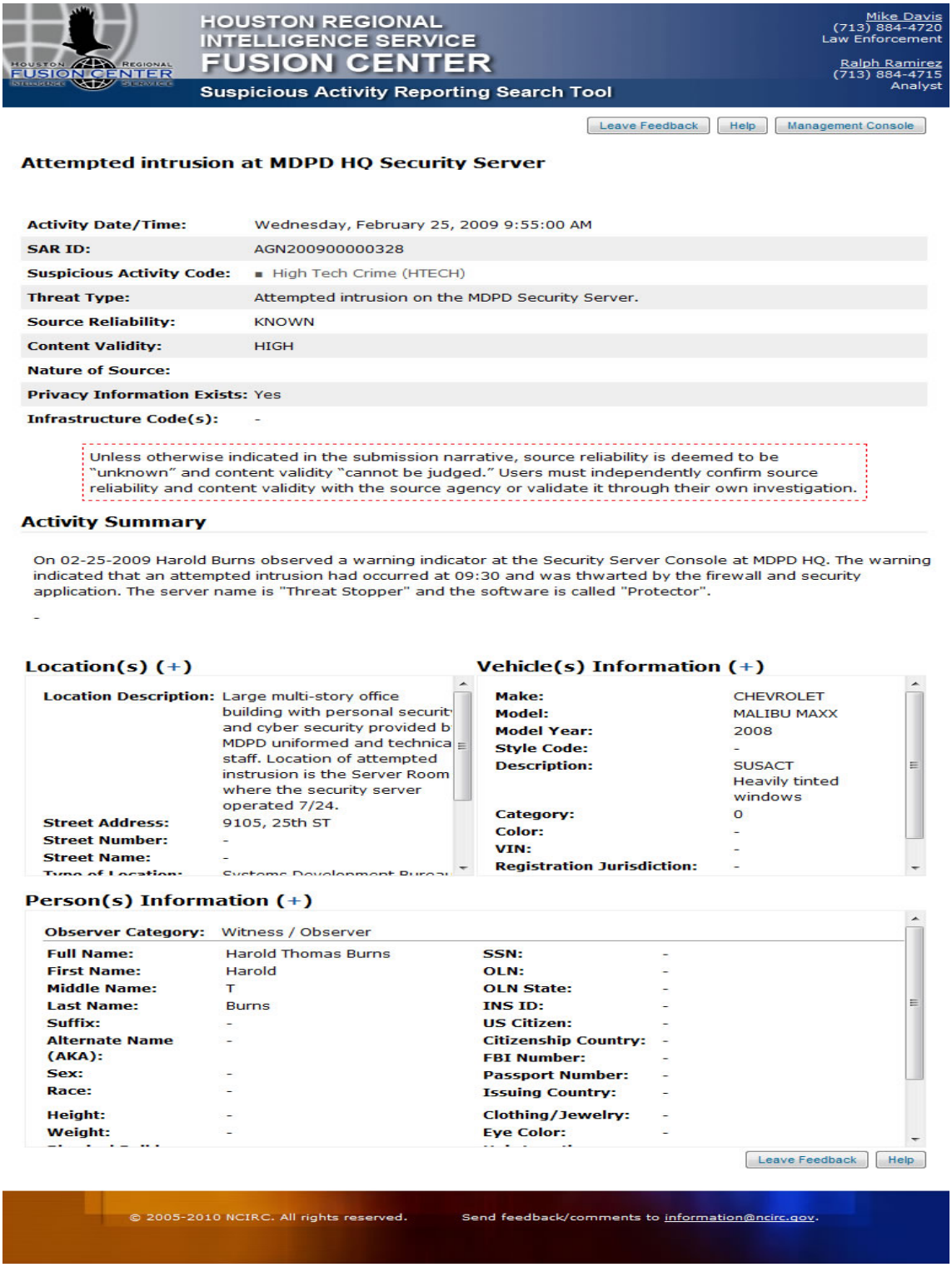

Figure 10. NSI Search Tool Detail SAR Report Screen

In addition to the NSI Search Tool accessed on the NCIRC site, the NSI PMO is offering fusion centers the SAR Vetting Tool (SVT) software application. The SVT was originally conceived by Fusion center staff in Chicago, Boston and Miami-Dade as a necessary tool to assist them in the vetting and submission of SARs for the NSI. The SVT is now deployed as part of the overall NSI Shared Space environment at seven fusion centers (as of March 2010). The following screen shots illustrate some of the SVT functionality

Figure 11 represents one of numerous screens supported by the SVT. In this example, the suspicious activity is documented on the Activity Tab. Other tabs are available to support information regarding Location, People and Vehicles plus a robust workflow process to allow Analysts and Supervisors to process the SAR reports that will be loaded into the fusion centers NSI Shared Space database. It's important to note that the SVT will allow for electronic input of SAR records from other systems if data is available. Fusion Center analysts would then update the imported data to add necessary codes or privacy fields that may be needed before selected SARs are forwarded to the Shared Space database.

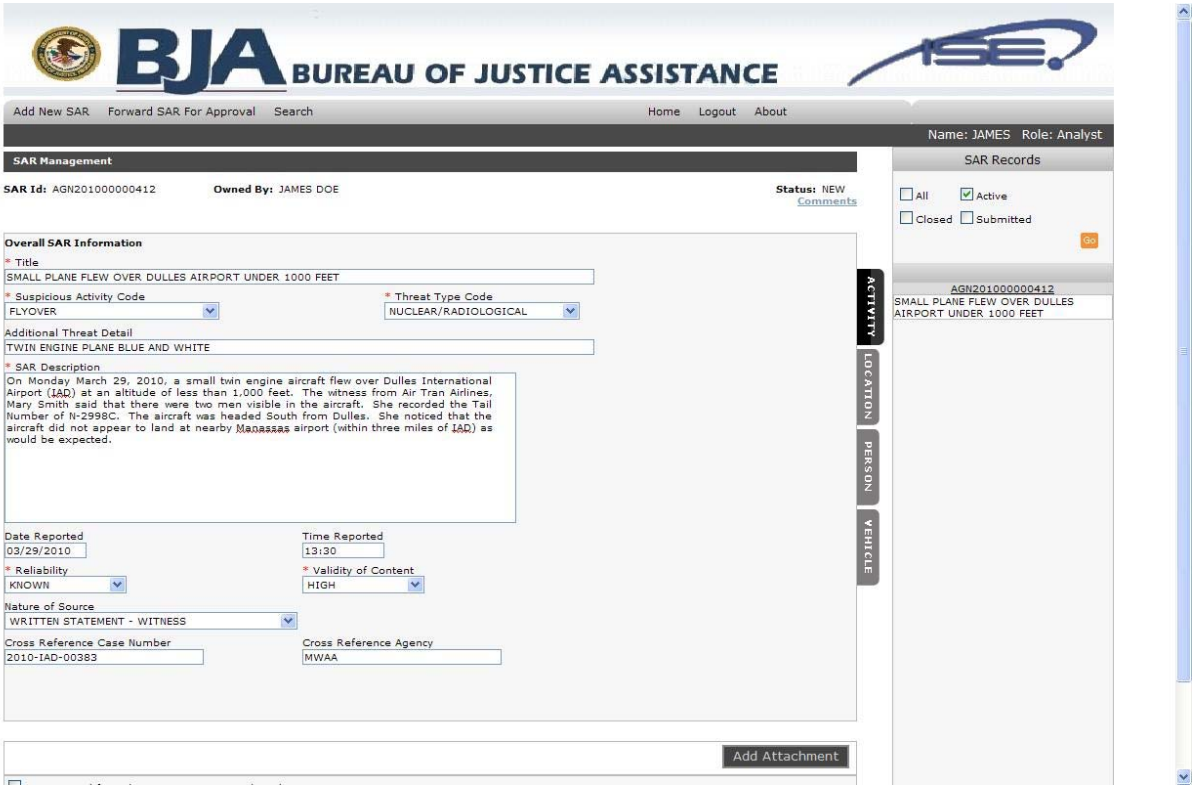

Figure 11. Sample SVT Screen

Comprehensive User Manuals for both the NSI Search Tool and the SVT are available upon request from the NSI PMO.