SERRI Report 89920-01

Multistate Sharing Initiative—Transportation Corridor Final Report

Project Principal Investigator:
Cyrus M. Smith

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 89920-01

SERRI Project: Transportation Corridor

MULTISTATE SHARING INITIATIVE— TRANSPORTATION CORRIDOR FINAL REPORT

Prepared by

Cyrus M. Smith
David E. Hill
Thomas B. Boehmann

Oak Ridge National Laboratory

Date Published:

October 2010

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

CONTENTS

ACRONYMS AND ABBREVIATIONS

ALPR	automatic license plate reader
CVIEW	Commercial Vehicle Information Exchange Window
DHEC	Department of Health and Environmental Control
DNDO	Domestic Nuclear Detection Office (DHS)
FMCSA	Federal Motor Carrier Safety Administration
IT	information technology
LEIC	Law Enforcement Information Center
MDOT	Mississippi Department of Transportation
ORNL	Oak Ridge National Laboratory
PRND	preventive radiological/nuclear detection
RPM	radiation portal monitor
RIID	radioactive isotope identification detector
SETCP	Southeastern Transportation Corridor Pilot (DNDO)
SERRI	Southeast Region Research Initiative
SFTP	Simple File Transfer Protocol
SLED	South Carolina Law Enforcement Division
SSH	Secure Shell
STP	State Transport Police
VPN	virtual private network
WIM	weigh-in-motion

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.

1. INTRODUCTION

The Southeast Region Research Initiative (SERRI) program allocated funding to The Oak Ridge National Laboratory (ORNL) to support the states of Mississippi and South Carolina in their commercial vehicle safety and compliance enforcement efforts.

This funding has enhanced three aspects of commercial vehicle law enforcement:

- inspection station information,
- radioactive isotope identification using handheld detectors, and
- automated safety and compliance scanning of commercial vehicles using automatic license plate readers.

The project was executed in two phases.

1. Phase I
   a. Storage and Internet Accessibility of Inspection Station Data
   b. Transmittal, Storage, and Internet Accessibility of radioactive isotope identification detector (RIID) Data from an Officer on Patrol
2. Phase II
   a. Real-Time Vehicle Checks of Commercial Vehicles

Mississippi and South Carolina inspection stations were chosen for this project for several reasons. Both of these states have participated in the Department of Homeland Security's Domestic Nuclear Detection Office's (DNDO's) Southeastern Transportation Corridor Pilot (SETCP) project, have radiation detection equipment provided by SETCP, have inspection stations that are modern enough to support the SERRI deployment, and have pledged complete cooperation in the execution of this project.

The Mississippi inspection station selected for this project is located in Kewanee, Mississippi, on I20/I59 (near the Alabama border). The South Carolina inspection station is located on I26 near Holly Hill, South Carolina (southeast of Orangeburg, in Orangeburg County).

SERRI has previously funded research conducted with the Kentucky Intelligence Fusion Center to integrate information from multiple commercial vehicle inspection stations within a state to yield insight into possible terrorist use of vehicles. The SERRI Transportation Corridor project continues the advancement of these technologies and transplants the technologies to the states of Mississippi and South Carolina.

2. PROJECT DESCRIPTION

2.1 Phase I—Storage and Internet Accessibility of Inspection Station and RIID Data

Phase I of the project enhances the states' existing commercial vehicle law enforcement efforts and complements their preventive radiological/nuclear detection (PRND) programs by providing a system to collect, store, and securely access inspection station data. This document will refer to this system in general as the Law Enforcement Information Center (LEIC) system.

The LEIC system has a graphical information system display module which will show a map of the state with the location of the fixed inspection station and the current or last known location of officers equipped with RIIDs and laptop computers with wireless Internet access.

Features of this system include the following.

- Storage of and secure Internet access to data collected at the inspection station.
- Encrypted transmittal, storage, and secure Internet accessibility of RIID data from an officer on patrol.

2.1.1 Inspection Station Data

DNDO has provided Mississippi and South Carolina radiation portal monitors (RPMs) as part of the SETCP project. This system includes a local display server to collect data for each commercial vehicle passing through the RPM. The inspection station data includes information about the truck, driver, and cargo. A truck observation record is created in the SETCP computer database at the inspection station. Date and time of the observation are collected along with vehicle images, a radiation "profile" of the truck, and alarm status; license plate images and optically read automatic license plate reader (ALPR) data are automatically generated. Manual entry of the driver's cargo manifest, spectral data from the RIID, and alarm resolution information are added by the law enforcement officer at the inspection station.

2.1.2 Mobile RIID Data

Any South Carolina State Transport Police (STP) officer equipped with a radiation pager and RIID can use this feature of the LEIC system. While the radiation pager is a standalone unit used to alert the officer when in the vicinity of a radiation field, it has only an audible output. The RIID can be used to locate and identify specific radioactive isotopes. Spectral data from the RIID can be further analyzed by radiation experts for more precise identification.

South Carolina STP patrol vehicles are typically equipped with a laptop computer with cellular data modem capabilities. A "client" software program must be installed on the laptop to facilitate uploading the spectra and additional commercial vehicle inspection information. The client software guides STP officers through the input and transmittal screens to input information and send it back to the LEIC system. With a Global Positioning System receiver, the officer's location can be automatically uploaded with the inspection information.

The Mississippi Department of Transportation (MDOT) did not wish to use the mobile RIID features described above.

2.1.3 The LEIC Viewer

Regardless of whether the data are collected at the inspection station or by an officer using the mobile RIID client, a data viewer is available for data sharing with other law enforcement officers, state Homeland Security personnel, and/or other state radiation health personnel. With this support, an officer can reach out to a local radiation expert (typically

someone within the state's health department) for help in determining the significance of the radiation that he detects while he is still in the field with the suspect vehicle.

There are two ways to view the data from the LEIC system, a web-based viewer and a mobile-client-based viewer. The web-based viewer can be used from any Internet connected computer using Microsoft's Internet Explorer or Mozilla's Firefox web browsers. The user will be challenged for appropriate security credentials. The web-based viewer is capable of read only viewing of the data and does not support data entry or RIID spectra uploading.

The mobile client viewer is typically used by the mobile officer using a handheld RIID. It does allow data input and RIID spectra uploading. The mobile client viewer supports manifest scanners, camera image uploading, and notes and comments as well as the radiation data.

Officers stationed at the inspection stations will use the SETCP viewer for all local truck observations and data uploads. If data from other sites need to be viewed, the officer can use the web browser and the LEIC viewer.

2.1.4 Planning and Installation and Server Hardware and Software Requirements

ORNL worked closely with Mississippi's and South Carolina's information technology (IT) personnel and chief information officers in the planning and deployment of the hardware and software components of this system. ORNL made recommendations and offered to procure the specific hardware, software, and operating systems required for these systems. The states' IT personnel and contracts departments were consulted prior to purchase to ensure proper ownership of the provided hardware. The states' IT personnel installed the operating systems and application software with ORNL providing guidance and technical support. This ensured that the states' cyber security requirements, including domain configuration and authentication, were properly followed. Each state's IT department was responsible for providing network infrastructure including adequate network bandwidth, clean power, air conditioning, and virtual private network (VPN)/firewall hardware and virus protection software. South Carolina provided their existing laptops and other hardware including cellular modems for the mobile RIID application.

Figure 1 refers to South Carolina's system topology; however, the topology for both systems is identical.

Users on the left side of the illustration would use the web-based read only viewer. They might include South Carolina STP officers, South Carolina Law Enforcement Division staffers, South Carolina Department of Health and Environmental Control personnel, or South Carolina Highway Patrol and Fusion Center personnel. Users on the right are data producers but may also be data consumers. They would include inspection station officers or mobile officers with the RIID mobile client. South Carolina STP and the inspection station systems are part of the South Carolina Department of Public Safety network. "Others" illustrated here are projected future users such as local fire/hazmat responders or federal agencies in support of the state's PRND program.

The two server system is used to separate the database from the web browser. Separating the database with a firewall makes the database more secure from internet cyber attacks. The web server runs Oracle's JAVA and Apache's Tomcat applications. The database server hosts a MySQL database for housing Commercial Vehicle Information Exchange Window (CVIEW) System data.

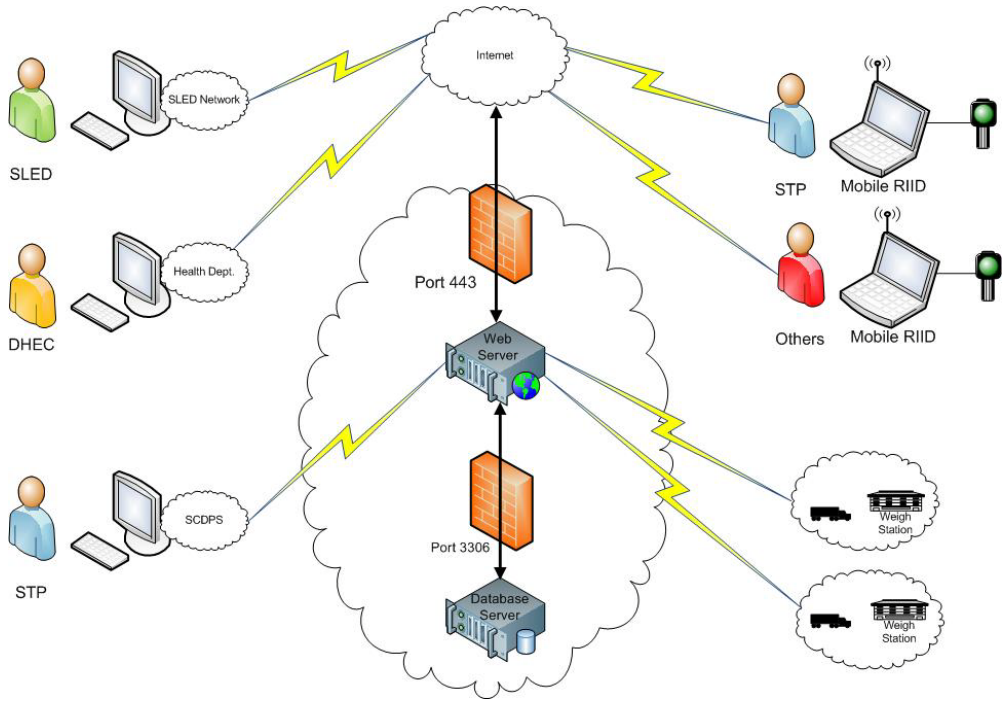


Figure 1. South Carolina's system topology.

2.2 Phase II—Real-Time Vehicle Checks of Commercial Vehicles

Phase II began with the installation of the ALPR on the entrance lane of a comercial vehicle inspection station. PIPS Technology's ALPR camera was chosen for the deployment; however, any ALPR vendor that supports the File Transfer Protocol could have been used.

2.2.1 Deployment

Deployment of this system began with the point to point fiber optic network (Figure 2). The fiber optic network connects the ALPR camera, located at or near the weigh-in-motion (WIM) system, to the Ethernet network port of the computer inside the inspection station. In Mississippi, it was possible to use existing dark fibers that were used for the WIM system. In South Carolina the DOT electricians ran the fiber optic cabling. (See Appendix A for the network topology.)

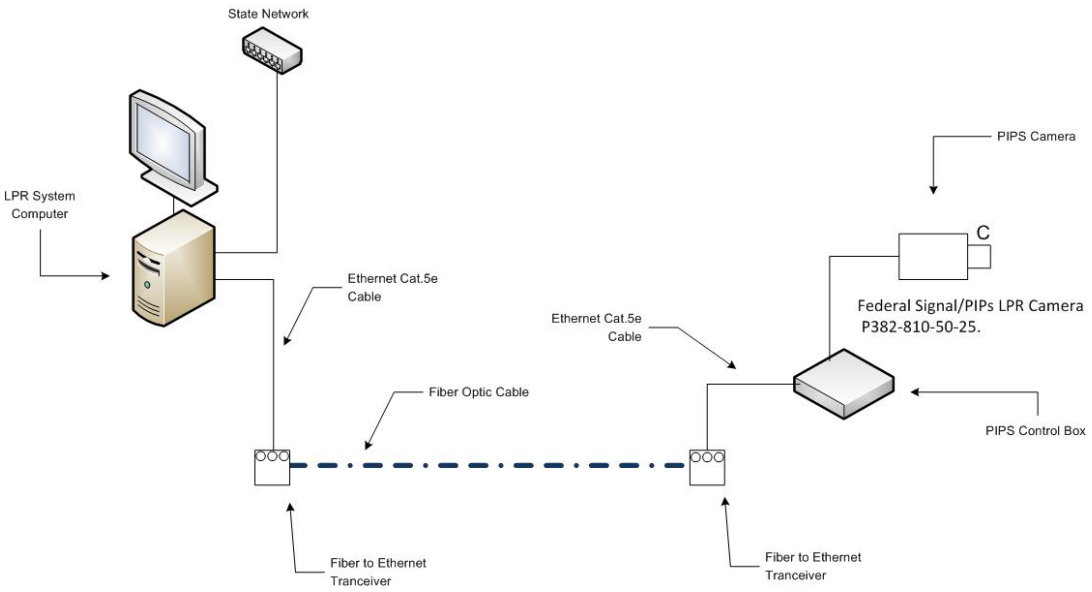


Figure 2. Point to point fiber network layout.

Camera installation was the next step (Figure 3). PIPS Technology provided the recommended installation instructions and alignment procedures.

Figure 3. Installation and alignment of the PIPS ALPR camera.

Computer setup consisted of installing the hardware and software and configuring the system.

The ALPR system developed by ORNL is a prototype system. The life expectancy of this system is 2 to 3 years. This time period is based on expected technology advances in electronic hardware, operating systems, and application software. It is no guarantee or warranty of performance or operation.

The system is designed to be self-maintained by MDOT/South Carolina STP and serviceable by the appropriate hardware vendors. The computers and monitors were purchased with a 3 year on-site warranty. PIPS Technology's ALPR cameras have a 1 year warranty, with an additional year for mail-in hardware parts and labor support. If PIPS is required to service on-site, MDOT/South Carolina STP will negotiate and provide financial support for the labor/travel expenses for PIPS personnel.

Service or repair to the fiber optics connectors, media converters, or fiber cable is the sole responsibility of MDOT/South Carolina STP. ORNL provides phone support at a best effort level, but additional funding for on-site support and repair maybe required.

2.2.2 Operation

The ALPR system automatically checks all vehicles passing through the inspection station instead of only the small percentage of vehicles passing over the static scales. Working in tandem with the ALPR results viewer, the ALPR camera can provide officers with indications of potential violations in near real time.

The violations are "potential" because the ALPRs are not able to read the state of issuance for a vehicle's license tag. The software checks the tag number from all possible states and alerts if there are any possible violations. The law enforcment officer is responsible for verifying that the tag number and state actually match that of the violation indication (Figure 4).

When the violation alert is given, the state scale specialist or law enforcement officer can manually trigger the control signals to move the vehicle to the static scales for further inspection. The violation alerts are not tied into the signal lights to direct the driver to pull over for inspection. Tying them together was considered, but it was felt that there is a lot of potential to overwhelm the law enforcement officers and cause an unsafe condition for both the officers and the commercial vehicle drivers. Because the states have indicated some interest in tying the alerts to the signal lights, commercialization of this project may include a private company working with the WIM vendor to accomplish this.

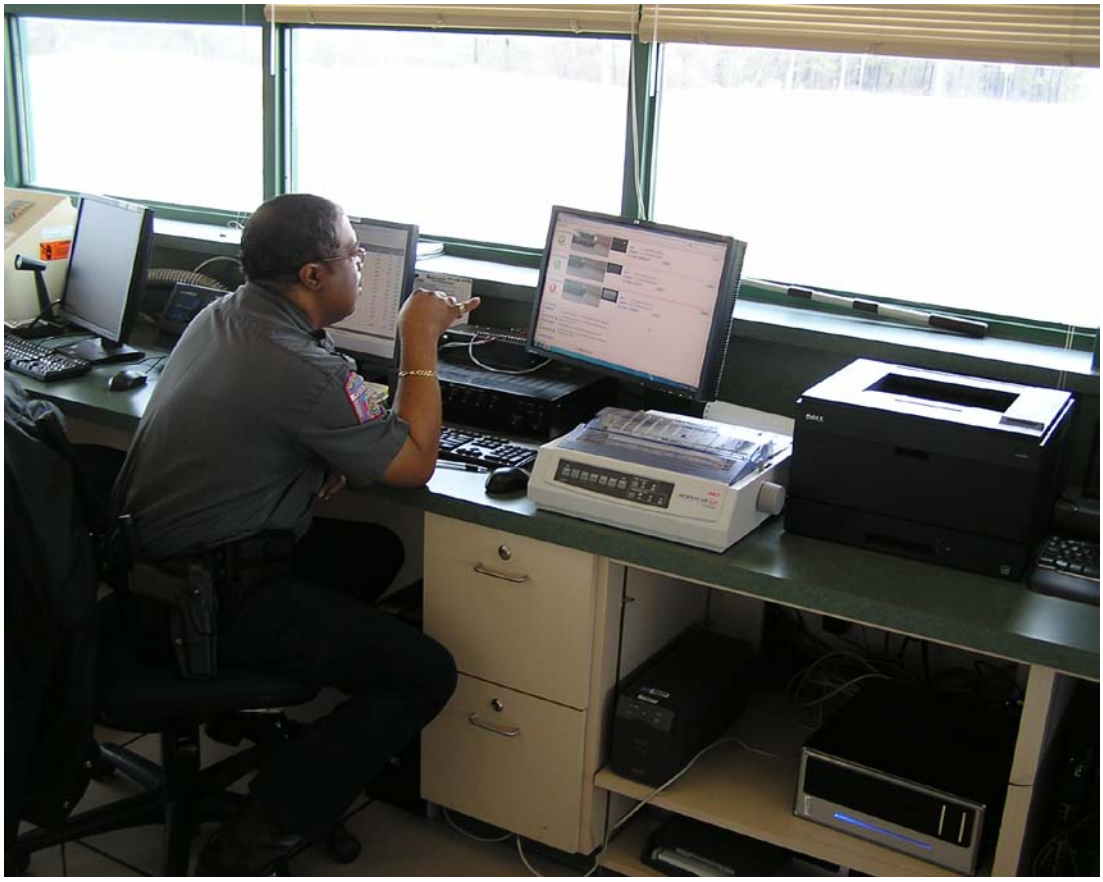


Figure 4. MDOT officer studying a violation alert.

As the truck goes through the inspection station a photograph of the license plate is acquired by the ALPR, and optical character recognition is used to identify the license plate number from the photograph. After the plate number is identified, a confidence number is assigned to the plate number according to how accurate the system's read is estimated to be. This information is then compared to the CVIEW database (see Section 2.2.3) for potential violations.

Violations checked by the CVIEW database include the following.

- Trucks on the National Crime Information Center stolen vehicle file
- Vehicles sanctioned by the Federal Motor Carrier Safety Administration (FMCSA) Performance and Registration Informatin System Management Program
- Expired registrations
- Unsatisfactory safety ratings
- Drivers declared out of service by FMCSA
- Unified Carrier Registration program
- Liability insurance
- Safety Status Measurement System category
- FMCSA out-of-service notices

2.2.3 Trusted Corridor CVIEW Data

A local copy of a subset of the CVIEW database is used to check for safety and other violations. The screening data itself is held in a local database for two reasons: (1) intermittent network connectivity or lost network connectivity will not impact the normal system operation (i.e., trucks can still be screened) and (2) the screening process needs to be as fast as possible to allow time for the truck driver to have time to react to a signal to pull into the static scale lane for verification and inspection.

The introduction of a local copy of the CVIEW database raises the issue of keeping the local database screening data up to date. Mississippi and South Carolina have a contract with Iteris, Inc., to provide them CVIEW data in a flat format file to be applied to the local MySQL database. ORNL worked with Iteris to develop a mechanism for refreshing the data on a regular basis. Other CVIEW data providers could also be used as long as the XML file structure matched the SERRI format.

When the system is initially installed, a series of baseline CVIEW data files are downloaded from the CVIEW data provider. A tool exists to load these baseline files into the local inspection station database. The baseline files follow the same file structure as the update files. Every night, the system at the inspection station will connect to a Simple File Transfer Protocol (SFTP) server and download the update files to apply to the local database. The system is configurable to accept an SFTP server's Internet Protocol address, port, user name, Secure Shell key, and server path. Using these configuration variables, the server will connect to the SFTP server, get a listing of relevant files to process, process each file, and delete each processed file. To ensure multiple stations can operate without conflicting, each inspection station has its own directory path and update files to process.

State administrators are given daily feedback as to how many commercial vehicles have been checked. The system sends a daily report to an email distribution list every evening at midnight (Appendix B). This report includes vehicle counts; the potential violations from the last 24 hours, last 7 days, and last 30 days; and an indication that the system is working properly. These reports may not reflect the exact number of vehicles that have passed through the inspection station as tags that are unreadable are not counted. License tags that are read are checked against the CVIEW database. In the event that an ALPR incorrectly reads a license tag, the law enforcement officer can correct the number by retyping the license tag number. The system then automatically performs a recheck and provides an update using the correct reading.

The viewer can also be used remotely as long as the user is resident on the local network. With this capability, an officer could use a tunneling tool such as VPN and a cell modem to monitor traffic from a police cruiser.

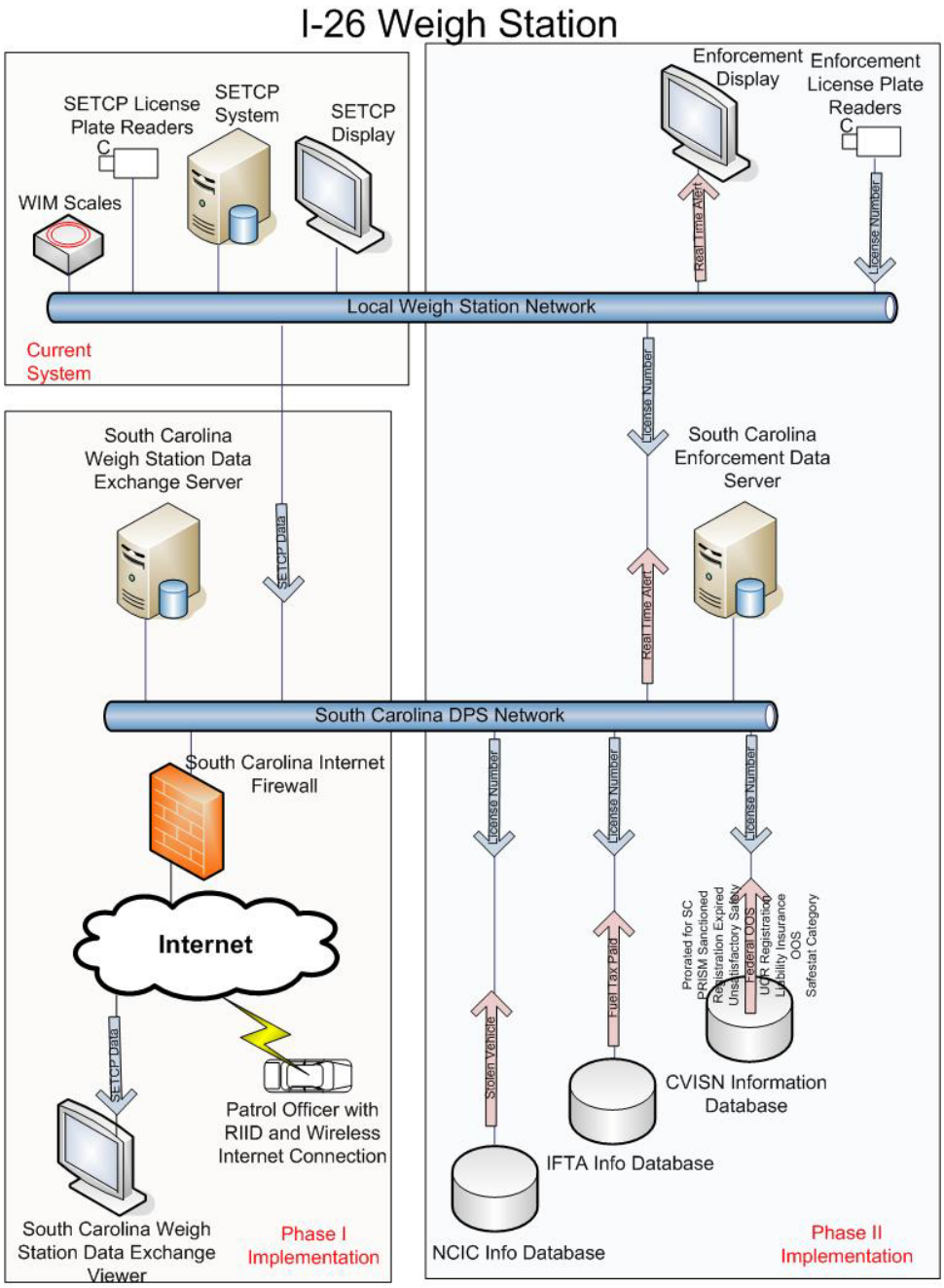
3. COMMERCIALIZATION

Teknas, Inc., (http://www.teknas.com) and Cadre5 Inc. (http://www.cadre5.com) have aligned to obtain the software copyrights to market the ALPR system. They are actively pursuing business opportunities for these technologies.

4. CONCLUSION

The SERRI systems were well received by both Mississippi and South Carolina. The ALPR system was especially well received as it almost instantly identified potential violations that can lead to revenue for the states. The ALPR system automatically checks well over 10,000 trucks per week per state and has the potential to be self supporting with the enforcement revenue that is generated. Mississippi and South Carolina are currently embarking on deploying the ALPR system throughout their states.

APPENDIX A. NETWORK TOPOLOGY



APPENDIX B. DAILY EMAIL REPORT

Kewanee EB Daily ALPR Report
Sun Aug 22 00:00:00 CDT 2010

Category	Past 24 Hours	Past 7 Days	Past 30 Days
Num Inspections	1,423	12,988	57,484
NCIC hits	0	1	5
PRISM hits	25	404	1,896
Expired registration	51	552	2,456
Unsatisfactory safety	0	6	16
Fed OOS	0	6	23
SafeStat A	4	46	220
SafeStat B	15	209	920
SafeStat C	11	140	617
All OOS > 75%	5	35	116
Vehicle OOS > 75%	3	44	170
Driver OOS > 75%	3	16	47
Hazmat OOS > 75%	0	24	109
Liability insurance violation	47	678	2,802
UCR not paid	0	0	0