Commercial Vehicle Information Systems and Networks (CVISN) National Program Management Plan

prepared by

Federal Motor Carrier Safety Administration
Technology Division

December 2007

draft report

Commercial Vehicle Information Systems and Networks (CVISN) National Program Management Plan

prepared by

Federal Motor Carrier Safety Administration
Technology Division

date

December 2007

Table of Contents

List of Tables

List of Figures

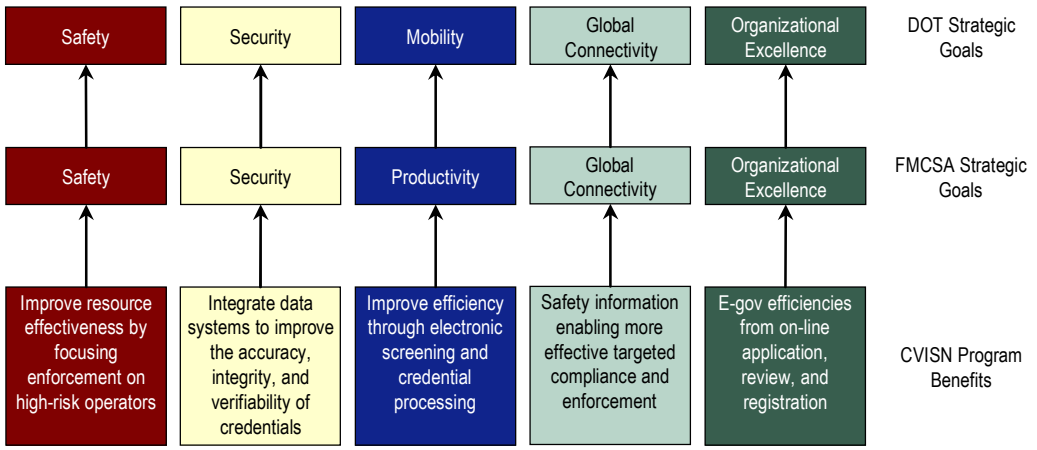
1.0 Introduction

The Commercial Vehicle Information Systems and Networks (CVISN) program is a key component of the Federal Motor Carrier Safety Administration's (FMCSA) drive to improve commercial motor vehicle safety. The program is directly aligned with both the United States Department of Transportation's (U.S. DOT) and FMCSA's strategic goals, which have been established in five areas. These areas are:

- Safety;
- Security, preparedness, and response;
- Reduced congestion;
- Global connectivity; and
- Organizational excellence.

As illustrated in Figure 1.1, the CVISN program supports these goals by focusing safety enforcement on high-risk operators; integrating systems to improve the accuracy, integrity, and verifiability of credentials; improving efficiency through electronic screening of commercial vehicles; and enabling on-line application and issuance of credentials.

Figure 1.1 CVISN Compliance with U.S. DOT and FMCSA Goals



1.1 SAFETEA-LU

The Safe, Accountable, Flexible, Efficient Transportation Equity Act – A Legacy for Users (SAFETEA-LU), a highway reauthorization act, was enacted on August 10, 2005 as Public Law 109-59. This legislation authorized $100 million in Federal deployment funds to support states' implementation of Core and Expanded CVISN functionality.

SAFETEA-LU authorizes the U.S. DOT to provide up to $2.5 million (less the amount of Federal Deployment monies a state received for its CVISN program under the Transportation Equity Act for the 21st Century – TEA-21) to each state for the deployment of Core CVISN capabilities. SAFETEA-LU also authorizes U.S. DOT to provide states up to $1 million in Federal Deployment Grants to support the states' deployment of Expanded CVISN capabilities. States that are certified as Core CVISN Compliant and have received less than $2.5 million in Federal Deployment funds can use the remainder of these monies to deploy additional Core or Expanded CVISN capabilities – if funds are available.

1.2 ORGANIZATION OF DOCUMENT

This document describes how FMCSA manages the Core and Expanded components of the CVISN program. The following sections are included in this document:

- **Section 1.0 –** Provides an introduction to CVISN and SAFETEA-LU;
- **Section 2.0 –** Documents the Core and Expanded CVISN capabilities and the stakeholder input process used to refine the Expanded CVISN capabilities;
- **Section 3.0 –** Documents the formulas that are used to calculate states' eligibility for Federal Core and Expanded CVISN Deployment Grants. This section also documents the match requirements for the Federal deployment funds and the FMCSA grant management process that is used to distribute the CVISN funds;
- **Section 4.0 –** Describes the process by which FMCSA ensures states' compliance with the CVISN program and its architecture;
- **Section 5.0 –** Documents FMCSA's CVISN communication and training plan;
- **Section 6.0 –** Summarizes the roles and responsibilities of FMCSA and its public and private sector partners; and
- **Appendix A –** Lists the Expanded CVISN capabilities that were previously identified by stakeholders.

2.0 CVISN Capabilities

2.1 CORE CVISN CAPABILITIES

The Core CVISN program is focused on three program areas. These areas are:

- **Safety Information Exchange –** designed to assure the safety of motor carriers, commercial vehicles, commercial drivers, and cargo through improved data collection and enhanced data sharing (inspection reports, credentials status, etc.). Projects within this area include automated roadside vehicle and driver inspections, and safety information systems that support the sharing of data across agencies and jurisdictions.
- **Electronic Screening –** designed to facilitate the verification of a commercial vehicle's size, weight, safety, and credentials information. Projects in this area include the use of transponder-based systems to identify commercial motor vehicles while in motion. Vehicles are allowed to bypass an inspection/weigh station as long as they are within size and weight restrictions, have the necessary operating credentials, and are operated by a motor carrier with a history of good safety performance.
- **Electronic Credentials Administration –** designed to automate the application, processing, and issuance of commercial motor carrier operating credentials and permits. Projects in this area automate the issuance of International Registration Plan (IRP) and International Fuel Tax Agreement (IFTA) credentials, as well as the processing of IFTA tax payments. Projects in this area also support the reconciliation of IRP and IFTA fees/taxes that are collected by one jurisdiction on behalf of another jurisdiction.

Each program area consists of core functionality that a state is required to deploy. This core functionality includes the following capabilities:

- **Safety Information Exchange**
  - Use ASPEN or equivalent automated inspection software at all major inspection sites;
  - Connect to the national Safety and Fitness Electronic Records (SAFER) system to exchange interstate carrier and vehicle safety data among states; and
  - Implement a state-specific Commercial Vehicle Information Exchange Window (CVIEW) system (or the equivalent) to store intrastate data and deliver interstate information to SAFER.
- **Electronic Screening**

  - Implement electronic screening at a minimum of one fixed or mobile inspection site, and be prepared to replicate this functionality at other sites.

- **Electronic Credentials Administration**
  - Automate processing of IRP and IFTA credentials;
  - Participate in the IRP Clearinghouse to share information across jurisdictions and automate funds settlement between jurisdictions; and
  - Participate in the IFTA Clearinghouse to share information across jurisdictions and automate funds settlement between jurisdictions.

All 50 states and the District of Columbia have begun to deploy some of the Core CVISN capabilities. When a state has deployed all of the Core CVISN capabilities, it is referred to as "Core CVISN Compliant." As of November 2007, 16 states are Core CVISN Compliant. In addition to the Core CVISN functionality, FMCSA and its state and industry partners have identified Expanded CVISN functionality that is being integrated into the CVISN program. The Expanded CVISN capabilities are described in Section 2.2.

2.2 EXPANDED CVISN CAPABILITIES

In order to further improve commercial motor vehicle safety and security and to extend the services provided through CVISN, FMCSA and the CVISN stakeholder community have identified a set of Expanded CVISN capabilities. These capabilities are designed to:

- Enhance the safety, security, and productivity of commercial vehicle operations; and
- Improve the access to, and quality of, information about commercial drivers, carriers, vehicles, chassis, cargo, inspections, crashes, compliance reviews, and citations for authorized public and private sector users.

The development of these capabilities has been guided by the lessons learned from the Core CVISN deployment program, advances in technology, and the increased focus on freight security and commercial motor vehicle drivers.

The Expanded portion of the CVISN program is designed to be more flexible than the Core component of the program. States are not required to deploy a set of fixed capabilities but rather may choose the capabilities that they wish to deploy. This "cafeteria approach" allows the states to customize their Expanded CVISN programs and focus their resources on the projects that are most important to them and their constituencies.

FMCSA, in conjunction with public and private stakeholders, initially identified 40 capabilities that could be integrated into the CVISN program.[1] These capabilities were segmented into four Expanded CVISN program areas:

- Driver Information Sharing;
- Enhanced Safety Information Sharing;
- Smart Roadside; and
- Expanded Electronic Credentialing.

The vision of each program area is summarized in Table 2.1.[2]

Table 2.1 Expanded CVISN Program Areas and Vision

Expanded CVISN Program Area	Vision
Driver Information Sharing	• Driver identification is consistent, reliable, and secure. • There is no commercial driver license (CDL) fraud. Each licensed driver is well-qualified to drive the commercial vehicles specified on his/her license, and no driver holds multiple licenses. • Driver privacy rights are protected, without compromising safety. • Authorized users (e.g., law enforcement, licensing agencies, potential and current employers) can easily access information about an individual driver. All authorized users access the same data source. • Future consideration: Authorized law enforcement personnel know who is driving a vehicle in advance of its arrival at an inspection site, port of entry, or other checkpoint and can more easily assess compliance with regulations.
Enhanced Safety Information Sharing	• Safety information is accessible through electronic means by authorized stakeholders. • Safety information is exchanged on intrastate and foreign carriers, as well as on interstate carriers. • Safety data quality is dramatically improved. • Law enforcement officers at all levels in all jurisdictions electronically submit and view inspection, crash, and citation reports from the roadside in a timely fashion.
Smart Roadside	• Safety, security, effectiveness, and productivity of roadside operations are improved through automation and application of proven technologies and processes. – Data collected by on-board systems are used to streamline and improve operations and enforcement activities. – Enforcement activities are conducted more effectively and frequently.

[1] A list of the 40 capabilities is included in Appendix A.

[2] FMCSA, Expanded CVISN Stakeholder Voting Results from the Commercial Vehicle and Freight Mobility (CVFM) Forum, September 2004.

Expanded CVISN Program Area	Vision
	– Safe and secure cargo moves efficiently through designated trade corridors. Intrusions and anomalies are detected. – Shippers, carriers, and customers can reliably predict the transit time for a given shipment and can check on its current status. – Enforcement knows which carriers, vehicles, drivers, or cargoes are high-risk and allocates resources accordingly.
Expanded Electronic Credentialing	• Motor carriers use convenient, fast, and accurate electronic methods to apply for, pay for, and receive all available e-credentials paperlessly through one portal (i.e., point of access). • Credentialing data is entered only once, by the authoritative originator, and re-used by all systems that need it. • Enrollment/application processes share common data elements and are consistent with state and Federal e-business practices and rules. • Paperless e-credentials are available for all authorized users, with near-real-time update and data correction capability. • CVO information systems support uniform, reliable, and complete data exchange standards for all identified credentials. • 100 percent of credentials will be issued to drivers, vehicles, and carriers who are compliant with all applicable regulations and laws and who are not security risks. • Consistent performance measures for cost, compliance, and data reliability are established to guide implementation of e-credentialing.

FMCSA presented the initial list of Expanded CVISN capabilities to a series of stakeholder groups, including representatives of the motor carrier industry, and asked that the stakeholders vote to identify the eight capabilities that they deemed most important to commercial vehicle safety, security, and productivity. Table 2.2 provides a brief description of each of the high-priority capabilities identified by the stakeholders.

At FMCSA's ITS/Commercial Vehicle Operations (CVO) Deployment Showcase in February 2005, FMCSA organized four working groups to further refine the Expanded CVISN capabilities. One group was assigned to each of the four Expanded CVISN program areas. The working groups were tasked with recommending solutions and deployment approaches for each high-priority capability. The working groups met through a series of conference calls during the spring and summer of 2005 and prepared a report for each of the capabilities. Each report included recommendations, a concept of operations, high-level requirements, potential solution alternatives, a rudimentary cost-benefit analysis, a business case, issues, and a deployment strategy. The recommendations are summarized in the Stakeholder Recommendations section below.

Table 2.2 High-Priority Capabilities Descriptions

Program Area	Capability	Description
Driver Information Sharing	Diver Snapshot	Establish, maintain, and provide controlled access to driver snapshots. Use and maintain driver snapshots in all processes (e.g., enforcement, credentialing, hiring, inspection) that require information about drivers.
	Access to Driver Data	Improve enforcement personnel and carrier access to driver information to target driver safety risks.
Enhanced Safety Information Sharing	Safety Data Quality	Establish data quality measures (timeliness, accuracy, and integrity), especially for those data elements used in determining ratings or making decisions. Regularly check data used in CVISN processes for quality; purge stale data; repair errors.
	Carrier Access to Safety Data	Improve a carrier's ability to review safety-related data (carrier, vehicle, driver, cargo, crash, citation, inspection) collected by a state or Federal agency in a timely manner. Consider proactively delivering safety data to the carrier.
Smart Roadside	Roadside Access to Data	Provide integrated and improved access for roadside personnel to data stored in infrastructure systems (e.g., SAFER, Motor Carrier Management Information System (MCMIS), CDL data systems).
	Virtual Roadside Sites	Expand the use and capabilities of virtual/remote sites to increase the effectiveness of enforcement.
Expanded Electronic Credentialing	Access to Credentials Data	Enhance interfaces and systems for information sharing to provide improved access to more current and accurate credentials information for authorized stakeholders.
	Better E-Credentialing	Reduce complexity and redundancy for users by offering access to multiple credentials from a single source. Users enter information once instead of multiple times. Increase the kinds of e-credentials that are available (e.g., add oversize/overweight [OS/OW] and hazmat permitting).

Stakeholder Recommendations

The Expanded CVISN working groups prepared a report for each Expanded CVISN program area, which summarized their recommendations to FMCSA. A series of general CVISN recommendations also were identified by the working groups. These recommendations include:

- Complete the deployment of Core CVISN functionality;
- Focus on quality of shared information;
- Capture lessons learned and best practices;
- Expand/improve data access;

- Improve roadside operations; and
- Maintain communication with stakeholders.

The working groups' specific recommendations are summarized below.

Driver Information Sharing Recommended Solutions

The Driver Information Sharing Working Group recommended that FMCSA consider a driver snapshot capability that would replicate a limited set of driver data in a central repository. This data would be stored for roadside screening and would build upon Core CVISN capabilities and interfaces. This working group also recommended that FMCSA establish a facilitated centralized driver data query that would build on the capabilities and interfaces available through Query Central and Commercial Driver License Information System (CDLIS). The working group also recommended consideration of a hybrid approach – combining the first two solutions.

The working group noted that while the sharing of driver data is important to improve safety and security, the privacy concerns of drivers also must be respected. The group recommended that representatives from the industry and government work together to mitigate the risks associated with the sharing of driver information. Working group members also noted that the development of a "driver safety rating" is critical to improving safety, security, and productivity. Members cautioned FMCSA that before embarking on any particular driver information sharing approach, stakeholders should agree on specific data elements, definitions, syntax, format constraints, and semantics that explain the intended business use of the data elements for each destination system and user type. This collaboration early in the process will help prevent duplication of efforts and incompatibility of emerging technologies.

Enhanced Safety Information Sharing Recommended Solutions

The Enhanced Safety Information Sharing Working Group provided recommendations regarding *Safety Data Quality* and *Carrier Access to Safety Data*. The working group recommended that a standardized approach for data sharing be established. Ideally this standard would account for an alignment of business processes, universal data dictionary, common identifiers, structure, protocols, and improved constraint checking. These stakeholders also suggested that access to safety data for carriers through a single Web portal (e.g., a one-stop shop for safety data) would improve efficiency. The working group recommended developing a capability to notify carriers when new data are posted to their safety records.

In addition to the above recommendations, this working group noted that data quality improvements should be part of every Expanded CVISN solution being considered. The group also advised that efforts to standardize information sharing should be coordinated with related initiatives both within and outside the transportation realm (e.g., Department of Justice).

Smart Roadside Recommended Solutions

The Smart Roadside Working Group recommended that the Expanded CVISN program include *Improved Roadside Access to Data* and *Virtual Roadside Site capabilities*. The working group encouraged FMCSA to augment/improve the data currently available at the roadside and to migrate from multiple stand-alone systems to a web-based solution. The group also recommended that FMCSA gather and disseminate best practices regarding access to, and display of, information at the roadside.

The working group recommended that Expanded CVISN should include virtual roadside sites. Moreover, the working group recommended that FMCSA play an active role in supporting the development of these sites. Specifically, the stakeholders recommend that FMCSA:

- Identify best practices and develop design and deployment templates for states to use in developing virtual roadside sites;
- Develop and encourage the adoption of standards to identify key entities (e.g., carrier, vehicle, driver, cargo) on the road; and
- Research and test emerging technologies.

The Smart Roadside Working Group also suggested that stakeholders should agree on specific data elements, definitions, syntax, format constraints, and semantics that explain the intended business use of the data elements for each destination system and user before FMCSA embarks on improving access to information from the roadside. The stakeholders noted the need for additional research on techniques to identify the carrier, driver, vehicle, and cargo at mainline speed. The working group also stated that although virtual roadside sites are established locally for a variety of purposes depending on the priorities and needs of each jurisdiction, FMCSA should continue to support these important safety/enforcement activities.

Expanded Electronic Credentialing Recommended Solutions

The Expanded Electronic Credentialing Working Group identified two key capabilities for improving e-credentialing in Expanded CVISN. *Access to Credentials Data Capability* would:

- Provide on-line access to Heavy Vehicle Use Tax (HVUT) payment status; and
- Require SAFER to provide better access to credentials data.

Better Electronic Credentialing Capability would:

- Reduce complexity and redundancy for motor carrier users by offering access to multiple credentials from a single source;

- Allow users to enter information once instead of entering it multiple times; and
- Expand the kinds of credentials that can be obtained electronically.

Recognizing that FMCSA's direct role in credentials administration is limited, the stakeholders recommended that FMCSA support the states' deployment of these capabilities by gathering and disseminating best practices information, exploring electronic payment mechanisms, and developing a benefit/cost framework.

This working group also recommended setting aside some portion of available funds to address emerging issues. Further, this group suggested that either it or some similarly constructed group of representatives of CVISN-affected entities should be reconstituted annually to review issues and develop priorities for e-credentialing. The group also urged FMCSA not to limit the number of Expanded CVISN capabilities to be undertaken.

FMCSA Investment in Expanded CVISN

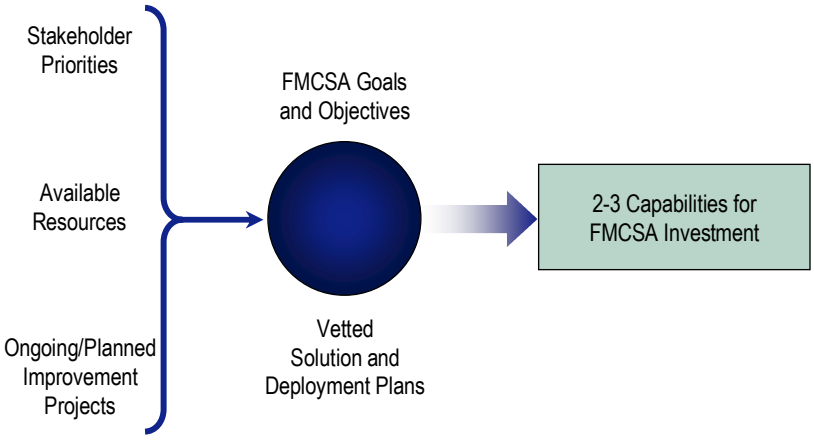
While states can deploy a wide variety of capabilities as part of their Expanded CVISN programs, FMCSA has decided to focus its resources on a limited number of key capabilities. FMCSA's support for these key capabilities includes architecture and standards development and maintenance, as well as formal training/technical assistance. States opting to implement an Expanded CVISN capability other than these high-priority capabilities are responsible (where applicable) for ensuring conformance with the national Intelligent Transportation Systems (ITS) and CVISN architectures, as well as guidance provided by FMCSA.

The input received from the CVISN stakeholders influenced FMCSA's investment decision. Other factors affecting FMCSA's investment decision included:

- **Scope –** FMCSA chose to focus on projects of national scope that required cross-jurisdiction coordination;
- **Organizational Priorities –** FMCSA's investment in Expanded CVISN needed to be consistent with the agency's overall safety mission;
- **Available Resources –** FMCSA's selection of capabilities was limited by available funding and staff resources; and
- **Ongoing Activities –** FMCSA's investment decision was influenced by ongoing related FMCSA activities (e.g., COMPASS, Comprehensive Safety Analysis [CSA] 2010, Wireless Bus, and Truck Inspections).

Figure 2.1 illustrates FMCSA's Expanded CVISN investment criteria.

Figure 2.1 Investment Decision Process



Based on its investment criteria, FMCSA chose to invest its Expanded CVISN resources in the Driver Information Exchange capabilities.

FMCSA chose to invest in the Driver Information Exchange area given the need for a national architecture to support the sharing of commercial driver data. The driver area also likely will have a large impact on commercial vehicle safety – given that high-risk drivers are involved in a disproportionate number of crashes. Finally, FMCSA chose to invest in this area because no other FMCSA program was designed to improve the sharing of information across jurisdictions.

Recommended capabilities related to improving roadside operations are being considered/addressed by a new program, the Smart Roadside Initiative.

3.0 CVISN Funding

Under the Safe, Accountable, Flexible, Efficient Transportation Equity Act – A Legacy for Users (SAFETEA-LU), U.S. DOT is authorized to issue grants to states in support of the states' deployment of Core and Expanded CVISN functionality. The legislation authorizes $25 million per year for a four-year period (Federal Fiscal Years 2006-2009) for this purpose. Under the legislation, FMCSA was given the discretion to determine how the $25 million will be divided among the CVISN components (Core and Expanded), as well as among the states. This document summarizes the following information for the Fiscal Year (FY) 2008 CVISN Deployment Grant Program:

- Funding Eligibility;
- Eligible Expenses;
- Schedule;
- Matching Funds;
- Application Process; and
- Available Support.

3.1 FUNDING ELIGIBILITY

SAFETEA-LU contains eligibility requirements that guide the distribution of Federal CVISN Deployment Grants. In accordance with these requirements, jurisdictions that want to apply for a FY 2008 Federal CVISN Deployment Grant to fund the deployment, operation, or maintenance of Core CVISN functionality must have:

- Completed a Core CVISN Program Plan and Top-Level Design and had the document(s) approved by FMCSA; and
- Received less than $3,500,000 in Federal CVISN funding in Federal Fiscal Years 1999 through 2007.

States that wish to apply for FY 2008 CVISN Deployment funding to support the deployment, operation, or maintenance of Expanded CVISN functionality must have:

- Been certified as being Core CVISN Compliant[3] or be able to demonstrate when they will be certified as Core CVISN Compliant;

[3] Being certified as Core CVISN Compliant by FMCSA indicates that a state has deployed all Core CVISN functionality.

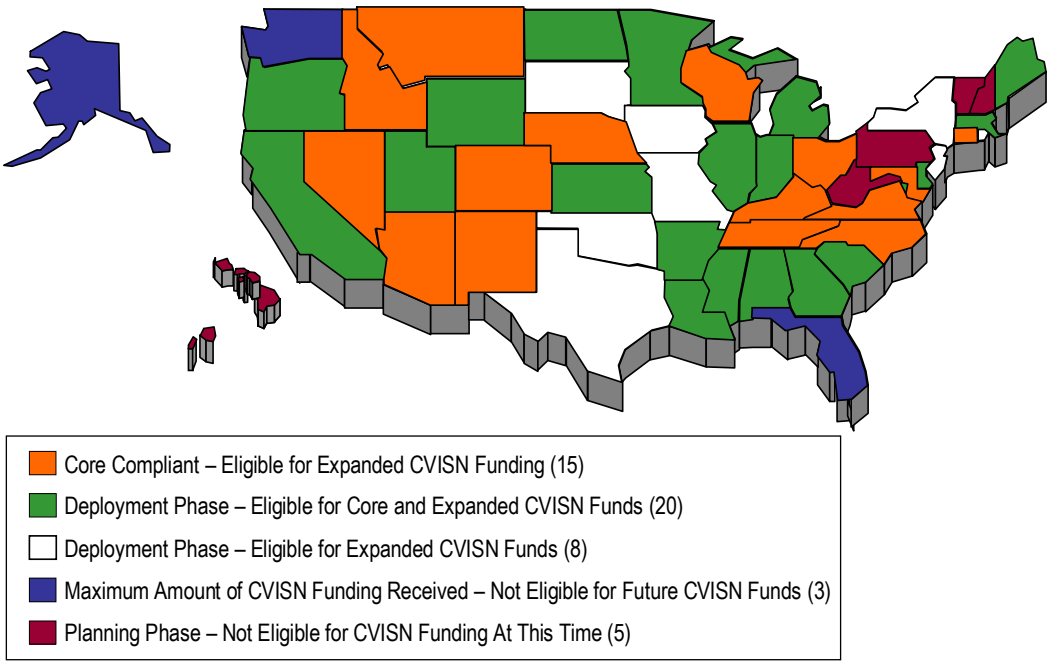
- Completed an Expanded CVISN Program Plan and Top-Level Design and had the document(s) approved by FMCSA; and
- Received less than $3,500,000 in Federal CVISN funding in Federal Fiscal Years 1999 through 2007.

As illustrated in Figure 3.1, five states currently are not eligible to apply for FY 2008 Federal CVISN funding because they have not completed a FMCSA-approved Core CVISN Program Plan and Top-Level Design.[4] Three states are not eligible to apply for future Federal CVISN funding because they have received the maximum amount of funding available to a single state under SAFETEA-LU ($3,500,000). As such, 43 jurisdictions (42 states and the District of Columbia) are eligible to apply for FY 2008 Federal CVISN Deployment funding.

States may apply to receive the maximum amount of CVISN funding for which they remain eligible under the guidelines contained in SAFETEA-LU. States will be informed of the specific amount of Federal CVISN funding for which they remain eligible via a letter from the FMCSA Administrator, which will officially kickoff the FY 2008 Federal CVISN Deployment Grant Program. Actual grant awards will be on a first come, first served basis, and are subject to the availability of FY 2008 funds.

[4] These states will become eligible for CVISN funding once they submit a Core CVISN Program Plan and Top-Level Design to FMCSA and the document is approved by FMCSA.

Figure 3.1 Summary of FY 2008 Federal CVISN Deployment Grant Eligibility[5]



3.2 ELIGIBLE EXPENSES

A state's current CVISN deployment status will determine the projects/expenses for which it may use FY 2008 CVISN Deployment funding. All states that are eligible to receive a FY 2008 CVISN Deployment Grant may use these funds to:

- Support CVISN program management (e.g., pay staff salaries, pay support/ advisory/administrative services);
- Pay ongoing CVISN-related operations and maintenance (O&M) expenses (e.g., system maintenance costs, system license fees); and
- Pay CVISN-related membership or program fees (e.g., e-clearance program fees, clearinghouse fees).

States in the Deployment Phase of their CVISN programs also may apply for a FY 2008 CVISN Deployment Grant to:

- Update their Core CVISN Program Plan and Top-Level Design (up to $100,000 of Federal CVISN Deployment funds may be used for this purpose);
- Deploy Core CVISN functionality in accordance with their FMCSA-approved CVISN Program Plan and Top-Level Design; and

[5] Data as of November 2007.

- At FMCSA's discretion, fund electronic credentialing projects beyond the automation of IRP and IFTA credentials (e.g., development of a one-stop shop/credentialing portal, automating the oversize/overweight permitting process, automating the intrastate credentialing process).

States that are certified as being Core CVISN Compliant or that can demonstrate when they will be certified as Core CVISN Compliant may apply for a FY 2008 CVISN Deployment Grant to:

- Develop their Expanded CVISN Program Plan and Top-Level Design(up to $100,000 of Federal CVISN Deployment funds may be used for this purpose);
- Complete their deployment of Core CVISN functionality;
- Augment their Core CVISN deployment (e.g., deploy a one-stop shop credentialing portal, offer electronic payment services);
- Address lingering concerns/issues associated with their Core CVISN deployment (e.g., address data quality concerns, improve timeliness of data sharing); and
- Deploy Expanded CVISN functionality (e.g., virtual weigh stations, driver-related capabilities).

Table 3.1 summarizes the eligible expenses for FY 2008 Federal CVISN funding.

Table 3.1 Summary of Eligible Expenses for FY 2008 CVISN Deployment Grants

State's CVISN Program Status	Eligible for Funds to Update Core CVISN Program Plan/Top-Level Design	Eligible for Funds to Deploy Core CVISN Functionality	Eligible for Funds to Develop Expanded CVISN Program Plan/ Top-Level Design	Eligible for Funds to Deploy Expanded CVISN Functionality	Eligible for CVISN-Related O&M Funds	Eligible for CVISN-Related Membership Fees
Planning Phase	No	Yes[a]	No	No	No	No
Core Deployment	Yes	Yes[b]	Yes[c]	Yes[d]	Yes	Yes
Core Compliant	No	No	Yes	Yes[e]	Yes	Yes
Maximum CVISN Funds Already Received	No	No	No	No	No	No

a Subject to FMCSA approving Core CVISN Program Plan/Top-Level Design.

b Subject to FMCSA approving updated Core CVISN Program Plan/Top-Level Design, if initial documents are out of date.

c Subject to state demonstrating when Core Compliance will be achieved.

d Subject to state demonstrating when Core Compliance will be achieved and FMCSA approving Expanded CVISN Program Plan/Top-Level Design.

e Subject to FMCSA approving Expanded CVISN Program Plan/Top-Level Design.

3.3 SCHEDULE

The FY 2008 CVISN Deployment Grant Program will be officially kicked-off in December 2007. Letters from the FMCSA Administrator will be sent to all states that are eligible to receive FY 2008 Federal CVISN Deployment funding. All applications for funding should be submitted to FMCSA by April 15, 2008. Should an applicant need additional time to complete his/her state's FY 2008 CVISN Deployment Grant application, he/she should contact Quon Kwan (quon.kwan@dot.gov) or Julie Lane (julie.lane@dot.gov) of FMCSA's Technology Division.

3.4 MATCHING FUNDS

Federal CVISN Deployment Grants require a dollar-for-dollar match. For instance, if a state is applying to receive a $1,000,000 FY 2008 CVISN Deployment Grant, it must identify $1,000,000 in matching funds. The matching funds must be derived from non-Federal (i.e., state or private sector) sources and must be related to the state's CVISN program. Allowable sources of match include:

- Cash;
- Contributions of equipment or facilities that are substantial and utilized entirely as an integral part of the state's CVISN program;
- Personnel services dedicated to the state's CVISN program for a substantial period and not supported by other Federal funds;
- Operations and maintenance expenses for CVISN-related systems, including vendor costs;
- Development expenses associated with CVISN-related systems, including vendor-paid costs;
- IRP/IFTA Clearinghouse fees; and
- E-clearance program membership fees.

When planning their matching funds, states should consider the following guidance:

- **Match may be accrued across a state's CVISN program.** For example, if a state is applying for a FY 2008 Federal CVISN Deployment Grant to deploy a Commercial Vehicle Information Exchange Window (CVIEW), the match for the grant need not be associated with the CVIEW project. The match could be generated by other projects within the state's CVISN program, such as the state's payment of the CVISN System Architect's salary or a private partner's investment in the state's electronic screening program.
- **Match is accrued over the life of the CVISN Program Agreement.** A state's match may be accrued over the life of the CVISN project/program (same as the period of performance stipulated in the CVISN Program Agreement) and

does not need to occur in the same fiscal year in which the Federal CVISN grant funds are expended. For instance, a state's match towards a CVISN Deployment Grant expended in FY 2008 to build a new CVIEW may include the purchase and set-up of hardware in FY 2009 on which the CVIEW software will be hosted.

- **In specific cases, match may be accrued prior to the CVISN Program Agreement's period of performance.** As a general rule, most expenditures made by a state grantee prior to the period of performance of a project may not be counted as credit for meeting the CVISN match requirements. An exception is payment for capital equipment or services i) that is made before the beginning of the period of performance of the CVISN project, but (ii) the capital equipment or services are used in the CVISN project during the period of performance of the CVISN project. In such a case, a prorated portion of the capital equipment or service expenditure may be counted as credit for meeting the CVISN matching requirements. For capital equipment, the prorated portion should take into account the useful life of the capital equipment and the rate of amortization (or depreciation). For services, the prorated portion should be based on the fraction of time that the services are used for the CVISN program. The guidance on capital equipment and services to be followed is the Office of Management and Budget (OMB) Circular A-87 and the "Common Rule" (also known as the "Uniform Administrative Requirements for Grants and Cooperative Agreements to State and Local Governments; Final Rule" at 49 CFR Part 19 (October 1, 1999)).

At this time, FMCSA continues to be unable to accept other Federal sources (i.e., Motor Carrier Safety Assistance Program [MCSAP], Performance and Registration Information Systems Management [PRISM], CDL, State Safety Data Improvement Program [SaDIP], Border) as match towards a Federal CVISN Deployment Grant. However, these sources may be used in conjunction with CVISN funds and allowable CVISN match to fund a project. For instance, Federal PRISM funds, Federal CVISN funds, and state funds (used to match the Federal CVISN funds) could be used to deploy a CVIEW. SAFETEA-LU mandates that the total Federal share of any CVISN project not exceed 80 percent.

Table 3.2 illustrates examples of allowable matches. Table 3.3 illustrates examples of unallowable matches, as well as the reason for the match being disallowed.

Table 3.2 Examples of Allowable Matching Fund Scenarios

Project Name	Total Project Value	FY 2008 Federal CVISN Grant Request	Matching Funds	Source of Match
Deploy a CVIEW	$150,000	$75,000	$75,000	State funds to purchase computer hardware on which CVIEW will be hosted.
Automate IRP Renewal Transaction	$500,000	$250,000	$250,000	State funds.
Fund Program Manager Salary (one-year)	$100,000	$100,000	$100,000	$100,000 in infrastructure improvements made at e-screening site by private sector partner.

Table 3.3 Examples of Unallowable Matching Fund Scenarios

Project Name	Total Project Value	FY 2008 Federal CVISN Grant Request	Matching Funds	Reason for Match Being Disallowed
Deploy a CVIEW	$100,000	$50,000	$50,000 (toll credits)	Toll credits currently are not an allowable source of match.
Automate IRP Renewal Transaction	$500,000	$300,000	$200,000	Insufficient matching funds identified.
Fund Program Manager Salary (one-year)	$100,000	$100,000	$100,000 (in MCSAP funding)	Other Federal programs cannot be used as match towards a CVISN grant.

3.5 APPLICATION PROCESS

In accordance with guidance from OMB, FMCSA is using the grants.gov web-based grant portal to disseminate and accept all FY 2008 grant applications – including those for CVISN. The FY 2008 CVISN grant package consists of two components – standard OMB forms and a CVISN-specific application in which

states will provide the necessary project detail (i.e., objectives, design, program compliance, schedule, and budget). Both portions of the FY 2008 CVISN grant package can be downloaded from the grants.gov web site. A user will be required to use the PureEdge Viewer from grants.gov in order to view and complete the OMB standard forms and to submit its completed application package. This PureEdge Viewer may be downloaded from grants.gov if a user does not have it.

Users that will be submitting a CVISN grant application must be registered with grants.gov as an Authorized Organizational Representative (AOR), someone who is legally authorized to submit a grant application on behalf of his/her agency. Once registered as an AOR, a state's CVISN representative will:

- Download the PureEdge Viewer from grants.gov;
- Log into grants.gov and download the CVISN application package and instructions;
- Complete the OMB standard forms (in PureEdge Viewer) and CVISN grant application (in Microsoft Word);
- Forward the CVISN grant application to the appropriate FMCSA Division Administrator (DA), in order to receive a preliminary review of the application's merits (e.g., are the proposed projects logical from a state/local perspective) and the appropriate application identifier number;
- Include the application identifier number (provided by the DA) on the standard forms and the CVISN grant application; and
- Log into grants.gov and upload the completed CVISN grant package (standard forms and Word-based application) to grants.gov via PureEdge Viewer.

Figure 3.2 illustrates the AOR registration process, as well as the CVISN grant application process being used in FY 2008. Training materials regarding the use of the grants.gov web site are available on the CVISN Collaboration SharePoint site: https://partners.jhuapl.edu/BA/hp/cvisn/CVISNGrants/FY08_grantsgov/Forms/AllItems.aspx. Table 3.4 summarizes the role of FMCSA Division Administrators and Headquarters staff related to the CVISN grant application process.

The application templates for the FY 2008 Federal CVISN Deployment Grant Program have been streamlined. States wishing to use FY 2008 funding only for O&M costs or planning expenses will be able to use templates designed specifically for these requests. Through the application process, states will be required to:

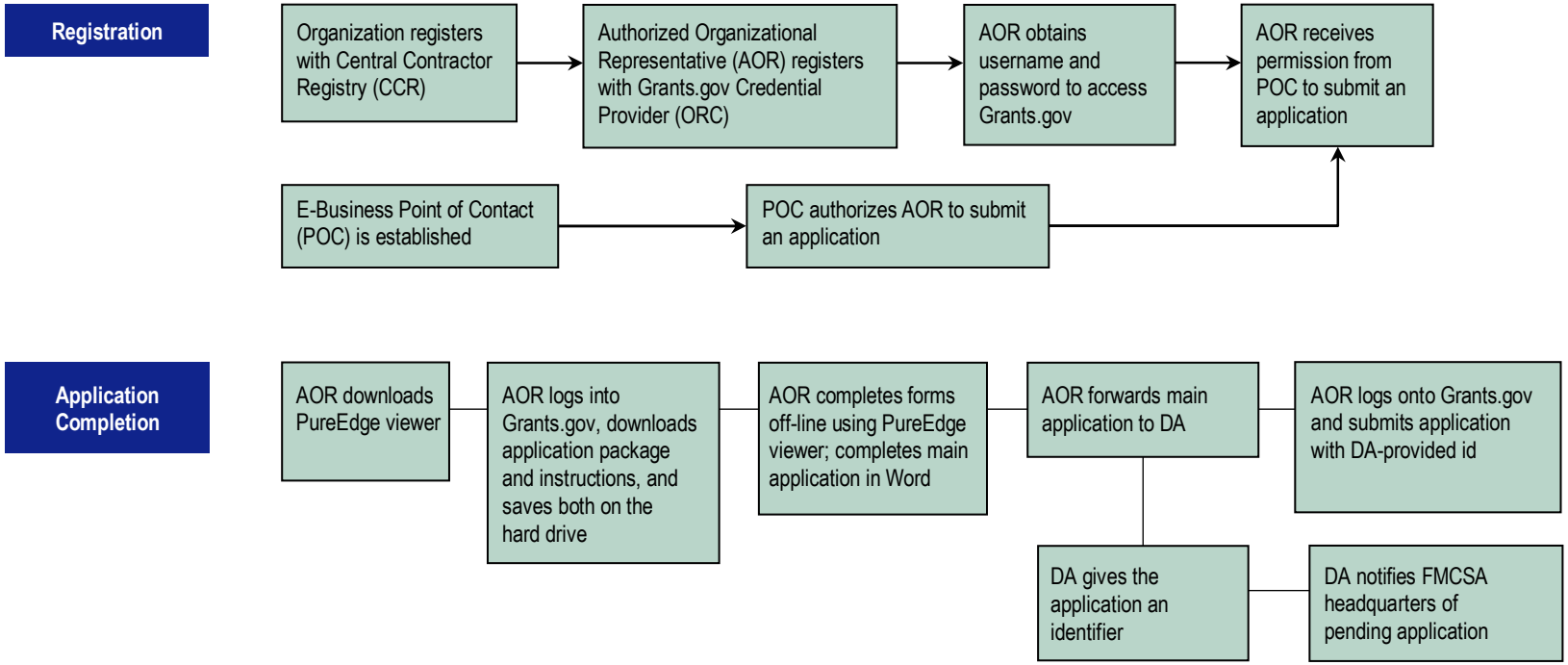
- Certify that their CVISN deployment activities are consistent with the national ITS and CVISN architectures and standards;

- Agree to execute interoperability tests developed by the FMCSA to verify that their systems conform with the CVISN architecture, standards, and protocols; and
- Agree to promote interoperability and efficiency to the extent practicable.[6]

States that are in the Planning Phase of their CVISN program are not eligible to receive CVISN Deployment funds until they prepare a Core CVISN Program Plan/Top-Level Design that is accepted by FMCSA. The CVISN program managers for these states should contact their FMCSA Division Administrator to arrange for FMCSA-sponsored technical assistance services (if needed) that will support the planning and documentation of their CVISN program.

[6] SAFETEA-LU, Section 4126(c)2.

Figure 3.2 Key Steps in Grant Application Process for States in Deployment Phase



Note: First check if agency is already registered. In that case, a POC already exists.

Table 3.4 Key Steps in Grant Application by Stakeholder

Responsible Entity	Step in Application Process
FMCSA Division Administrator	• Review state's Core and/or Expanded CVISN Program Plan/Top-Level Design documents. • Provide a preliminary review regarding the merits of his/her state's CVISN Deployment Grant application (e.g., are proposed projects logical from a state/local perspective). • Provide the appropriate state contact with the required CVISN application identifier number. • Receive final draft of CVISN Program Agreement from FMCSA HQ and forward it to state CVISN Program Manager for review. • Coordinate between the state CVISN Program Manager and FMCSA Technology Division regarding the state's comments to the CVISN Program Agreement (if necessary). • Ensure state's CVISN Program Agreement is signed by an authorized entity within the state. • Sign final version of state's CVISN Program Agreement. • Forward signed version of state's final CVISN Program Agreement to FMCSA HQ. • Notify the state CVISN Program Manager when the grant funds have been posted to the U.S. DOT Delphi accounting system and requests for reimbursement can be processed. • Notify the state CVISN Program Manager of the project code associated with the grant. • Review requests for reimbursements and indicate recommendation for payment. – Requests for reimbursements that have been recommended for payment may be optically scanned and e-mailed to the Federal Aviation Administration (FAA) Financial Operations/Accounts Payable Office (based in Oklahoma City) or sent to the FAA Liaison to FMCSA. • Continue to monitor the progress of the state's CVISN program and ensure that the state is fulfilling its portion of the match requirement. Also ensure that the state submits quarterly progress reports, as required by the CVISN Program Agreement.
FMCSA Headquarters	• Review and accept states' Core and/or Expanded CVISN Program Plan/ Top-Level Design documents. • Review a state's CVISN grant application package. • Draft a CVISN Program Agreement and obtain a legal review of the Agreement from FMCSA Office of Chief Counsel. • Forward final draft of state's CVISN Program Agreement to state's FMCSA Division Administrator. • Prepare a memorandum to request that the FAA Liaison to the FMCSA Financial Operations/Accounts Payable Office (MC-MBF) establish an

Responsible Entity	Step in Application Process
	obligation for the state (for the amount specified in the CVISN Program Agreement) in the U.S. DOT Delphi accounting system for the purpose of paying requests for reimbursement. The memorandum must be signed by the Director, FMCSA Office of Analysis, Research, and Technology and include the following: – Copy of the signed CVISN Program Agreement attached with the CVISN grant application; – Project code. The project code is assigned in accordance with the FMCSA Grants Management Manual; – Information about the state's grant recipient point of contact (name, address, and city); and – Copy of the completed automated clearinghouse (ACH) payment form (if the state is a new CVISN grant recipient or if a state desires to change the bank account into which reimbursement payments are directly deposited). • Send a copy of the FAA obligation request memorandum (with the signed ACH payment form, Grant Obligation Checklist, and a hardcopy of the CVISN Program Agreement with the original signatures as the only attachments) to FAA Accounts Payable Staff. • Check to see if the obligation has been posted in the U.S. DOT Delphi accounting system. • Notify the FMCSA Division Administrator when an account has been established in U.S. DOT Delphi accounting system for the grant funds.

Members of the FMCSA and FAA accounting and legal departments also will play key roles in the CVISN grant management process.

3.6 AVAILABLE SUPPORT

Reference materials and guidance documents (e.g., grants.gov instructions, examples of successful CVISN grant applications, FY 2008 grant application templates) have been posted to the CVISN Collaboration SharePoint site: https://partners.jhuapl.edu/BA/hp/cvisn/CVISNGrants/FY08_grantsgov/Forms/AllItems.aspx. The FMCSA CVISN Team also is available to answer states' questions about the FY 2008 CVISN Deployment Grant Program (e.g., would a project be eligible for funding via the grant program, how much funding is a state eligible to receive in FY 2008, how to identify eligible sources of matching funds). Further, FMCSA can make technical assistance services available to states, if necessary. Questions and requests for assistance should be directed to:

- Quon Y. Kwan
  Federal Motor Carrier Safety Administration
  Tel: (202) 385-2389
  E-mail: quon.kwan@dot.gov

- Julie Lane
  Federal Motor Carrier Safety Administration
  Tel: (202) 385-2391
  E-mail: julie.lane@dot.gov

4.0 Program Conformance

While the Expanded CVISN program is designed to be more flexible than the Core CVISN program, states are required to demonstrate compliance with the national program in order to be eligible for funding. States will be required to demonstrate both programmatic and technical/architectural conformance with the national CVISN program. This section summarizes how states currently are required to demonstrate their compliance with the Core and Expanded components of the CVISN program.

4.1 CORE CVISN PROGRAM CONFORMANCE

In accordance with SAFETEA-LU, states are required to prepare a Program Plan and Top-Level Design that is submitted to and approved by FMCSA in order to be eligible to receive Core CVISN funding. This document is a state's primary mechanism to demonstrate its intended compliance with the Core CVISN program. As part of the program planning process, a state must complete the CVISN Operational and Architectural Compatibility Handbook (COACH) checklists. COACH requires state CVISN program teams to consider various aspects of CVISN compliance (e.g., commitment to ITS/CVO Guiding Principles, inclusion of all required credentialing systems) and explicitly state their intent in the document to comply with these provisions. States also are required to comply with program requirements (e.g., reporting, independent evaluation, and self-evaluation) that are contained in its CVISN Deployment Program Agreement(s). Should a state's planned CVISN implementation fundamentally change or become dated, it is required to update its Program Plan and Top-Level Design and have the updated version of the document reviewed and accepted by FMCSA.

If a state indicates that it will be less than fully compliant with the COACH requirements, it is required to explain the business and/or technical rationale for their decision(s). FMCSA reviews all states' Program Plan and Top-Level Design documents. FMCSA may request that a state provide additional information about its exceptions to a COACH element. FMCSA reserves the right to withhold Core CVISN funding to a state that does not agree to all elements contained in COACH. To date, FMCSA has accepted the COACH documents from 46 states. FMCSA will support the remaining five jurisdictions as they complete the COACH documents and document their compliance with the CVISN program.

FMCSA also verifies a state's compliance with the technical architecture of Core CVISN through the SAFER Interface Certification Process. Before a state is allowed to upload data to the Federal SAFER system, it first must demonstrate its compliance with SAFER standards (e.g., format and content of pre-established message sets). If a state is not compliant with the SAFER interface standards, it is

not allowed to upload data to SAFER and therefore cannot be considered Core CVISN Compliant. If a state deviates from approved designs or interfaces after they are authorized to upload data to SAFER, the state must be re-certified as compliant via the SAFER Interface Certification Process. The CVISN Architecture Configuration Control Board (ACCB) is the mechanism by which states can request a modification to the CVISN architecture and/or systems.

4.2 EXPANDED CVISN CONFORMANCE

As with Core CVISN conformance, states are required to document their compliance with the Expanded CVISN program through an Expanded CVISN Program Plan and Top-Level Design document. Through this document, a state will document the current status of its CVISN program, what Expanded CVISN functionality will be deployed, and how the state will deploy it. FMCSA has developed a template to guide development of a state's Expanded CVISN Program Plan and Top-Level Design.

A state is required to document in its Expanded CVISN Program Plan/Top-Level Design, where applicable, how it plans to conform to the national ITS and CVISN architectures. For instance, states that wish to use Federal Expanded CVISN Deployment Grants to improve the sharing of driver information will need to commit to the use of a standard identifier for commercial drivers. These states also will need to commit to sharing the specified information in a standard format, including syntax, definition, and format.

While reviewing a state's Expanded CVISN Program Plan and Top-Level Design, FMCSA will determine if the state's level of commitment to the national architectures is sufficient. If a state is not sufficiently committed to complying with the national architectures, FMCSA will request changes to the state's Program Plan/Top-Level Design. If the state is unwilling or unable (e.g., business rules do not allow compliance) to modify its approach, FMCSA will not approve the state's Expanded CVISN Grant request.

Similar to states deploying Core CVISN functionality, states deploying Expanded CVISN functionality also will need to comply with program requirements (e.g., reporting, independent evaluation, and self-evaluation) that are contained in their CVISN Deployment Program Agreement(s).

5.0 Communication and Training

FMCSA employs a multifaceted communication and training plan to reach out to and educate internal FMCSA stakeholders, as well as public and private sector stakeholders, about Core and Expanded CVISN. This section summarizes FMCSA's approach to communication and training.

5.1 INTERNAL COMMUNICATION PLAN

Numerous FMCSA initiatives are directly related to CVISN and must be closely coordinated with the program. The primary FMCSA initiatives with which the CVISN program are coordinated include:

- **COMPASS –** FMCSA's program to consolidate and modernize its information systems. This program impacts all aspects of CVISN that rely on FMCSA's safety data systems (e.g., SAFER, MCMIS, ASPEN). This program also impacts the timeliness with which CVISN-specific requests are made to FMCSA's data systems.
- **Comprehensive Safety Analysis 2010 (CSA 2010) –** FMCSA's effort to "evaluate the effectiveness of its current safety compliance and enforcement programs, and identify better methods of achieving a crash-free environment."[7] This program affects FMCSA's and the states' enforcement model and may alter the roadside and safety data sharing components of CVISN.

Coordination meetings have occurred between CVISN and these other initiatives and will continue periodically and as necessary. An Expanded CVISN ad hoc team has been formed to provide a venue for CVISN stakeholders to be educated about and to provide input to the COMPASS program.

5.2 EXTERNAL COMMUNICATION PLAN

FMCSA will disseminate information to the various stakeholder groups and gather feedback on the program from the stakeholders. FMCSA's activities will leverage the stakeholder groups currently in place and streamline the process by which it disseminates information. The key elements of this plan include:

- **CVISN Program Managers' Conference Calls –** FMCSA convenes monthly conference calls among the state CVISN program managers. These calls are designed to update the program managers on key elements of the national

[7] Comprehensive Safety Analysis 2010 Listening Session Final Report. Touchstone Consulting Group, March 7, 2005. Page 1.

CVISN program, including funding eligibility and grant management requirements. These calls also serve as a forum for state CVISN program managers to exchange information among themselves and to solicit specific technical expertise and/or assistance from their peers. FMCSA uses these calls as a mechanism to request feedback on the CVISN program from the state program managers.

Since January 2006, these calls have been structured by state deployment status – as opposed to geography. Currently, two calls are held:

- States in the Planning and Deployment Phase of their Core CVISN program; and
- Core Compliant states participating in the Expanded CVISN program.

This new structure allows the calls to be tailored to meet the unique needs of each group of states. However, in order to facilitate dialogue among the states, all states will be able to participate in either of the calls.

- **Targeted State-Specific Communications –** FMCSA sends state-specific letters/e-mails to communicate information to the states, as needed and appropriate. For instance, FMCSA Administrator John Hill is providing state-specific letters to each jurisdiction eligible for CVISN funding, in order to encourage their participation in the CVISN Deployment Grant Program.
- **Ad Hoc Task Teams –** As needed, FMCSA will form ad hoc task teams to consider specific issues regarding the CVISN program or a specific capability. Each team will comprise CVISN stakeholders (e.g., state credentialing representatives, state enforcement personnel, motor carriers, motor coach operators, Federal staff, and insurance company representatives) with an interest in the team's topic. Three teams currently are discussing specific motor carrier issues. These teams include:
  - Coordination with the COMPASS Initiative;
  - Roadside identification of carriers, vehicles, drivers and cargo; and
  - Heavy Vehicle Use Tax (HVUT).

  The teams meet as needed and are supported by FMCSA and its CVISN program consultant support team.
- **ACCB Calls –** FMCSA conducts regular ACCB calls. These calls are designed to "review, analyze, discuss, and make recommendations about proposed changes to the CVISN architecture and generic Top-Level Design".[8]
- **Stakeholder Briefings –** FMCSA or stakeholder ad hoc team members deliver CVISN briefings to both public and private sector stakeholder groups.

[8] CVISN Architecture Change Management Process and SAFER/Federal System Change Management Process, July 2005.

The public-sector groups typically include Commercial Vehicle Safety Alliance (CVSA), American Association of Motor Vehicle Administrators (AAMVA), Intelligent Transportation Society of America (ITSA), and American Association of State Highway and Transportation Officials (AASHTO). Private sector stakeholder groups typically include American Trucking Associations (ATA), and ATA's Technology and Maintenance Council (TMC). These briefings provide an update regarding the status of the CVISN program, highlight accomplishments to date, and describe next steps. These briefings also provide an opportunity for the stakeholders to provide feedback to FMCSA regarding the CVISN program and any open/ outstanding issues that may exist.

- **CVISN Deployment Workshops –** FMCSA plans face-to-face CVISN Deployment Workshops in order to tackle deployment concerns and issues related to data integrity, data quality, and data availability, as well as to discuss common business rules related to maintenance and usability of the data that are exchanged via SAFER. In spring 2007, FMCSA held the first CVISN Deployment Workshop at the National Training Center in Arlington, Virginia. The workshop was a unique opportunity for FMCSA to meet in person with multiple state CVISN champions and work directly with them to resolve issues. A follow-up session is being planned for 2008.
- **CVISN Collaboration SharePoint Site –** FMCSA supports the operation of the CVISN SharePoint site, which is an on-line project collaboration facility. Through the CVISN SharePoint site, users can share/access relevant technical documents, access a CVISN-specific calendar of events, and be electronically notified of upcoming meetings and conference calls. The CVISN SharePoint Site has numerous sub-sections, including:
  - CVISN Calendar;
  - CVISN Document Library;
  - CVISN Deployment Grant Program;
  - CVISN Training;
  - CVISN Marketing;
  - ACCB;
  - CVISN/PRISM Deployments;
  - Core CVISN;
  - Expanded CVISN; and
  - One sub-section for each CVISN ad hoc team.

5.3 TECHNICAL ASSISTANCE PLAN

FMCSA is committed to providing members of state CVISN program teams with the necessary training to support their deployment of Core and Expanded CVISN capabilities. FMCSA provides formal training services in support of the Core CVISN program. FMCSA also makes customized technical assistance available to the states, in support of both the Core and Expanded CVISN programs. FMCSA's complete CVISN technical assistance plan includes:

- **Core CVISN Training Courses –** FMCSA-approved trainers deliver customized training courses to state CVISN program teams requiring a "refresher" on basic concepts and technical elements of the Core CVISN program. These courses are delivered at the request of a state CVISN program manager and/or a FMCSA Division Administrator. States interested in receiving training courses should contact their FMCSA Division Administrator who will coordinate with FMCSA Headquarters to deliver the needed services.
- **Core and Expanded CVISN Workshops –** FMCSA-approved trainers deliver streamlined on-site versions of the CVISN workshop series. These streamlined workshops are designed to focus on a state's CVISN organization and functional needs. The workshops support the development of a state's Core or Expanded CVISN Program Plan and Top-Level Design document. At FMCSA's discretion, states receive FMCSA support in developing their Program Plan and Top-Level Design. States interested in receiving this technical assistance should contact their FMCSA Division Administrator who will coordinate with FMCSA Headquarters to deliver the needed services.

In addition to these formal training activities, FMCSA will conduct a series of lessons learned, business cases, and best practices assessments to support states' Core and Expanded CVISN programs. FMCSA also convenes periodic conferences/showcases to highlight the leading Core and Expanded CVISN activities and provide an opportunity for information exchange between the various CVISN stakeholder groups. These activities are conducted by FMCSA staff, as well as support contractors.

6.0 Roles and Responsibilities

FMCSA and its public sector and private sector partners all play critical roles in ensuring the success of the CVISN program. Within FMCSA, the Office of Analysis, Research and Technology (ART), as well as the FMCSA Division Offices, are the primary organizations responsible for the CVISN program. The primary public and private sector stakeholders involved in CVISN are:

- Representatives from all state commercial vehicle-related agencies;
- Multi-state coalitions;
- Motor carrier and motor coach industries; and
- Private sector vendors/partners.

This section summarizes the primary responsibilities of each group.

6.1 FMCSA RESPONSIBILITIES

FMCSA has primary responsibility for the management and oversight of the CVISN program. FMCSA's ART is responsible for the following CVISN-related activities:

- Developing and maintaining the necessary architecture and standards to support the Core and Expanded components of the CVISN program;
- Coordinating monthly status calls with state CVISN program managers and system architects, as well as FMCSA Division Administrators (or designees);
- Issuing guidance to the FMCSA Division Offices and states regarding the Federal CVISN Deployment Grant Program and Expanded CVISN functionality;
- Determining the exact amount of funding for which a jurisdiction is eligible to apply for in a given year;
- Drafting the CVISN Program Agreement for the FMCSA Division Administrator to execute with the state;
- Reviewing and accepting the states' Core CVISN Program Plans and Top-Level Designs, in coordination with the FMCSA Division Administrators;
- Reviewing and accepting the states' Expanded CVISN Program Plans and Top-Level Designs, in coordination with the FMCSA Division Administrators;
- Providing technical assistance and training to FMCSA Division staff and states on Core and Expanded CVISN functionality;

- Supporting development of states' Core and Expanded CVISN Program Plans and Top-Level Designs;
- Monitoring deployment status and conformance with CVISN standards and architecture, as well as with the requirements contained in the states' CVISN Deployment Program Agreement(s);
- Developing performance measures to monitor the deployment and effectiveness of the Core and Expanded CVISN capabilities;
- Coordinating between CVISN and other FMCSA and U.S. DOT initiatives (e.g., COMPASS, CSA 2010);
- Facilitating an ITS/CVO national deployment showcase at least once every two years; and
- Conducting a bi-annual CVISN program review with key stakeholders to evaluate the effectiveness of the program.

The FMCSA Division Offices are responsible for:

- Reviewing and approving their state's Core CVISN Program Plan and Top-Level Design (if necessary);
- Reviewing and approving their state's Expanded CVISN Program Plan and Top-Level Design;
- Executing the Core and Expanded grants with the states; and
- Providing management oversight of their state's CVISN deployment program and managing their state's Federal CVISN Deployment Grant(s), including reviewing and approving interim products and vouchers.

6.2 STATE RESPONSIBILITIES

States are responsible for planning, deploying, operating, and maintaining their CVISN architecture and services. As part of their deployments, states are responsible for:

- Developing and maintaining a state-specific Core CVISN Program Plan and Top-Level Design that documents the Core CVISN functionality that will be deployed and how their state will deploy the Core CVISN architecture;
- Developing and maintaining a state-specific Expanded CVISN Program Plan and Top-Level Design that documents the business case for Expanded CVISN functionality, identifies the Expanded CVISN functionality that will be deployed, documents the state's Expanded CVISN design, details how the state will conform to the national ITS and CVISN architectures (where appropriate), and documents the state's Expanded CVISN deployment plan;
- Organizing and maintaining a state CVISN program team that includes representatives from all state agencies related to commercial vehicle

operations, as well as representatives from the motor carrier and motor coach industries;

- Ensuring their state's conformance with the national CVISN program's goals, objectives, architecture, and standards;
- Implementing their deployment plans (e.g., contracting or building in-house the required elements of the CVISN architecture);
- Managing the CVISN funding grant program, in conformance with procedures established by FMCSA;
- Conforming with FMCSA's financial reporting and accountability process and practices;
- Reporting their state's CVISN deployment status, in conformance with their CVISN Deployment Program Agreement(s);
- Completing annual updates to its CVISN self-evaluation;
- Collecting data in support of FMCSA's evaluation and performance monitoring requirements;
- Marketing their state's CVISN program and its associated services to the motor carrier and motor coach industries; and
- Participating in monthly calls with the FMCSA Division Administrator (or designee) and state CVISN program managers and system architects.

6.3 MULTI-STATE COALITIONS ROLE

Numerous multi-state coalitions (e.g., I-95 Corridor Coalition, Gary-Chicago-Milwaukee Corridor, and West Coast Corridor Coalition) have been designated as high-priority corridors by Congress. These coalitions share information among their members, organize state responses to FMCSA regulatory inquiries, and fund a variety of regional projects. With regards to the CVISN program, the multi-state coalitions will be responsible for:

- Serving as a testbed for CVISN projects of regional significance (e.g., vehicle identification, sharing of credential information, credential administration);
- Supporting their members' planning of CVISN deployments;
- Supporting the training of their members' CVISN program teams; and
- Coordinating stakeholder input regarding the CVISN program.

6.4 INDUSTRY ROLE

The motor carrier and motor coach industries are the primary users of the CVISN electronic screening and electronic credentialing services deployed by the states as part of the Core CVISN program. The industry also will be key users of the

driver data facility included in the Expanded CVISN program. These users also will be a key source of corrected safety data within FMCSA's information systems. Overall, the industry has the following CVISN-related responsibilities:

- Sharing their expertise and functional requirements with FMCSA and state CVISN teams;
- Participating in the stakeholder feedback mechanisms provided by FMCSA; and
- Using the Core and Expanded CVISN services provided by FMCSA and the states.

6.5 PRIVATE SECTOR ROLE

Public-private partnerships and private sector technology vendors are key elements of states' CVISN deployments. These entities provide funding, research, and innovation to the CVISN program. Their primary CVISN responsibilities include:

- Supporting states' CVISN deployments;
- Developing CVISN-compliant software and services;
- Participating in CVISN deployment showcases; and
- Sharing their expertise with FMCSA and state CVISN teams, as appropriate.

In addition, private consultants provide professional management and technical services to many states' CVISN programs, frequently serving as program management consultants and system architects to CVISN states.

Appendix A – Expanded CVISN Capabilities

Below is a listing of the 40 Expanded CVISN capabilities originally identified by FMCSA and the stakeholder community.

Driver Information Sharing

- Establish, maintain, and provide controlled access to driver snapshots/Use and maintain driver snapshots for all processes.
- Improve access to driver information for enforcement and carrier personnel to target driver safety risk.
- Provide roadside tools to evaluate compliance with hours of service regulation.
- Improve identity checks in all driver licensing processes.
- Link driver performance data to related carrier ID, in order to identify high-risk carriers.
- Determine security rating for drivers.
- Provide on-line tools to help carriers assess potential drivers and monitor current drivers' performance.
- Ensure that systems control access to driver records.
- Allow the driver to review, challenge, and correct information in their driving record.
- Expand the use of standards for CDLs and information systems that store driver data.
- Improve the standardization of citation data collection and information sharing among enforcement agencies.

Expanded Information Sharing

- Establish data timeliness, data accuracy, and integrity measures.
- Regularly check data used in CVISN processes for timeliness, accuracy, and integrity; purge stale data and repair errors.
- Expand core safety systems to include standard information storage and exchange for intrastate and foreign carriers, in addition to interstate carriers.
- Establish or expand "data stores" for cargo, carrier, vehicle, and driver credential, safety, and enforcement data.

- Provide on-line tools to enable appropriate users to provide timely information about corrections to deficiencies detected during inspections.
- Improve the carrier's ability to review safety data associated with its record/ Consider proactively delivering safety data to carrier.
- Provide on-line tools for law enforcement to submit crash reports and citation reports.
- Enable jurisdictions to maintain up-to-the-minute inspection history data.

Smart Roadside

- Expand access to data collected by on-board systems to improve roadside operations.
- Provide integrated and improved access for roadside personnel to data stored in core infrastructure systems (e.g., SAFER, MCMIS, CDL data systems).
- Provide carriers with streamlined and timely access to citation, crash, and inspection information so they are better informed about safety problems.
- Associate high-risk cargo with the container, chassis, vehicle/transponder, carrier, vehicle, and driver transporting it.
- Expand the use of standard electronic security devices (ESDs) to improve container and trailer security and reduce theft.
- Monitor status of the ESDs throughout the trip by collecting "event data" at toll booths, ports of entry, inspection/weigh stations, and freight yard entries/exits.
- Expand the use of technologies and processes to verify only authorized drivers and personnel are able to access the vehicle, trailer, and container.
- Provide access to the event data and related information to authorized private and public sector users – based on legitimate needs for information to improve productivity, streamline operations, and improve security.
- Expand the use of mobile data entry devices (e.g., laptop, personal data assistant [PDA], cell phone) and applications to improve data quality and streamline data collection.
- Expand the use and capabilities of virtual/remote sites to increase the effectiveness of enforcement.
- Expand the use of technology to generate real-time safety and security alerts.

Expanded e-Credentialing

- Reduce complexity and redundancy for users by offering access to multiple credentials from a single source.

- Increase the number e-credentials that are available (e.g., OS/OW permitting, hazmat).
- Offer a variety of standard e-payment options.
- Improve the process for enrolling in multijurisdiction programs (e.g., e-screening programs, e-toll) through provision of links.
- Provide for automated queries to cross-check supporting requirements across agencies, states, and Federal systems.
- Enable legacy credentialing systems to update CVIEW with changes in credentials data for real-time access.
- Enhance interfaces and systems for information sharing to provide improved access to more current and accurate credentials information for authorized stakeholders.
- Designate one authoritative source for each credential-related data element and provide date/time stamp.
- Use secure electronic identification, notification, documentation, and screening for vehicles, carriers, drivers, and cargo.
- Expand the set of standard data elements for information exchange related to credentials.