Intelligent Transportation Systems (ITS)
Commercial Vehicle Operations (CVO)

Commercial Vehicle Information Systems and Networks (CVISN)

Operational and Architectural Compatibility Handbook (COACH)

Part 1
Operational Concept and Top-Level Design Checklists

NSTD-08-487 V4.0

November 2008

This is Version 4 of a Baseline Issue

This document has completed internal and external reviews of previously published drafts and preliminary versions. All comments received to date have been incorporated or addressed.

Note: This document and other CVISN-related documentation are available for review and downloading by the ITS/CVO community from the Federal Motor Carrier Safety Administration (FMCSA) CVISN site on the World Wide Web. The URL for the CVISN site is: http://cvisn.fmcsa.dot.gov/.

Additional review and comments to this document are welcome.

Ms. Sandra B. Boys		Phone:	443-778-7610
The Johns Hopkins University		Fax:	443-778-6149
Applied Physics Laboratory		E-Mail:	sandra.boys@jhuapl.edu
11100 Johns Hopkins Road			
Laurel, MD 20723-6099			

Change Summary: This document is under configuration management by the CVISN Architecture Configuration Control Board (ACCB). See Appendix C for information concerning change requests (CRs) applicable to this version of the document.

CVISN Operational and Architectural Compatibility Handbook (COACH)
Part 1 – Operational Concept and Top-Level Design Checklists

Table of Contents

List of Tables

This Page Intentionally Blank

1. INTRODUCTION

The Commercial Vehicle Information Systems and Networks (CVISN) Operational and Architectural Compatibility Handbook (COACH) provides a comprehensive checklist of what is required to conform with the CVISN operational concepts and architecture. It is intended for use by state agencies with a motor carrier regulatory function. Other readers may include motor carriers and developers/operators of CVISN Core Infrastructure systems.

Reference 1, the *CVISN Glossary*, contains an acronym list as well as brief descriptions of many commonly used terms.

1.1 COACH Structure and Evolution

The COACH was originally divided into five parts:

- **Part 1 – Operational Concept and Top-Level Design Checklists**
- Part 2 – Project Management Checklists
- Part 3 – Detailed System Checklists
- Part 4 – Interface Specification Checklists
- Part 5 – Interoperability Test Criteria

The COACH documents supported the CVISN workshop series held in the late 1990s through 2003. This is the sixth revision to the *COACH Part 1*. *COACH Parts 2* through *4* have been archived and are available from the Federal Motor Carrier Safety Administration (FMCSA) by request. Most of the relevant information from those documents has been incorporated into the *COACH Part 1*, *CVISN System Design Description,* and *CVISN Architecture*. To gain a more complete understanding of CVISN, state planners and designers should read:

- *Introductory Guide to CVISN* [Reference 2]
- *CVISN System Design Description* [Reference 3]
- *CVISN Architecture (Revised)* [Reference 10]

COACH Part 5 is now obsolete. These documents should be referenced for interoperability testing:

- *COACH Part 1, Appendices A and B*
- *Safety and Fitness Electronic Records (SAFER) Interface Certification Procedure (ICP*), Version 1.0, July 2003 [Reference 4]
- *SAFER Commercial Vehicle Information Exchange Window (CVIEW) Interface Re-Certification*, Version 7, January 2008 [Reference 5]
- *SAFER CVISN State Data Baseline Procedure*, Version 1.0, March 2008 [Reference 6]

1.2 COACH Part 1 Description

The *COACH Part 1* defines the Core CVISN criteria. The document includes several types of checklists related to operational concepts and top-level design. This version of the document contains these chapters:

- Guiding Principles: high-level strategic guidelines [Chapter 2]
- State Institutional Framework Checklists: compatibility requirements for the policies and coordinating activities for states [Chapter 3]
- CVISN Operational Concepts and Top-Level Design Checklists: compatibility requirements for processes and top-level compatibility requirements for state designs [Chapter 4]
- Data Maintenance Requirements [Chapter 5]
- References [Chapter 6]
- Core CVISN Checklists [Appendix A]
- Recommended End-to-End Tests [Appendix B]
- Change Requests Incorporated into the Current Version [Appendix C]

1.3 Summary of Core CVISN Requirements

This section provides a simplified summary of Core CVISN criteria. Chapter 4 shows the details about what states must do to be Core CVISN compatible.

- **An organizational framework for cooperative system development has been established among state agencies and motor carriers.**
- **A state CVISN System Design has been established that conforms to the CVISN Architecture and can evolve to include new technology and capabilities.**
- **All the elements of three capability areas (below) have been implemented using applicable architectural guidelines, operational concepts, and standards:**
  - **Safety Information Exchange**
    - Inspection reporting using ASPEN (or equivalent) at all major inspection sites. ASPEN data sent to SAFER (Safety and Fitness Electronic Records) directly or indirectly.
    - Connection to the SAFER system to provide exchange of interstate carrier and vehicle data snapshots among states.
    - Implementation of Commercial Vehicle Information Exchange Window (CVIEW) (or CVIEW equivalent) system for exchange of intrastate and interstate data within state and connection to SAFER for exchange of interstate data through snapshots.

      – OR –

    - Utilization of SAFER option for exchange of inter- and intrastate data through snapshots.
  - **Credentials Administration**
    - Automated electronic processing via Web-based or computer-to-computer solutions from carrier to state (processing includes carrier application, state application processing, credential issuance, and tax filing) of at least IRP (International Registration Plan) and IFTA (International Fuel Tax Agreement) credentials; ready to extend to other credentials [intrastate, titling, OS/OW (Oversize/Overweight), carrier registration, HazMat (Hazardous Materials)]. Note: Processing does not necessarily include e-payment.
    - Update SAFER with credential information for interstate operators as actions are taken.
    - Update CVIEW (or equivalent) with interstate and intrastate credential information as actions are taken.
    - Connection to IRP and IFTA Clearinghouses.

- At least 10% of the transaction volume handled electronically; ready to bring on more carriers as carriers sign up; ready to extend to branch offices where applicable.

– **Electronic Screening**

- Use snapshots to support screening decisions.
- Implemented at a minimum of one fixed or mobile inspection site.
- Ready to replicate at other sites.

1.4 How States Should Use This Document

The COACH summarizes key concepts and architectural guidelines for CVISN in a series of checklist tables. The *COACH Part 1* checklists are intended to be used to indicate the scope and depth of CVISN commitment, and to provide a mechanism for planning development and test activities. The *COACH Part 1* is intended to be a working document that is used for setting requirements for modifications and enhancements to existing state systems, and for planning the development of new systems in states. Each state should maintain a filled-in master copy of the document. The checklists should be filled in initially during the CVISN program initiation phase, then revisited and updated periodically.

Each table in this document consists of these columns, unless otherwise noted:

- Commit Level (F/P/N) – the state's commitment level to the item

  Using the first column of each checklist entry, a **commitment level should be filled in** by the state. There are three possible levels of commitment:

  – (F) This rating indicates a full commitment. This level means that at least 80% of the state's systems involved in the process implied by the checklist item are compatible, or are intended to be compatible, with the checklist item statement.

  – (P) This rating indicates a partial commitment. This level means that between 50% and 80% of the state's systems involved in the process implied by the checklist item are compatible, or are intended to be compatible, with the checklist item statement.

  – (N) This rating indicates no commitment. This level means that less than 50% of the state's systems involved in the process implied by the checklist item are compatible, or are intended to be compatible, with the checklist statement.

- Item # – a label to identify each row in the table
- Compatibility Criteria – summary versions of operational concepts or architectural guidelines, culled from other CVISN documentation
- Req Level (Core/Expanded) (Chapter 4 only) – the compatibility requirement level assigned to this compatibility criterion by FMCSA

  For a state to be "compatible with CVISN," it must implement selected items in the checklists. To distinguish those items, FMCSA has assigned a **compatibility requirement level** to each checklist item:

  - (Core) This rating identifies a Core CVISN compatibility requirement.
  - (Expanded) This rating indicates an Expanded CVISN capability that a Core CVISN-compliant state may choose to implement.

  States are expected to focus initially on checklist items with a *Core* compatibility requirement level rating. Making a *partial commitment* indicates that the state will at least demonstrate the feasibility of that concept or architectural guideline. Making a *full commitment* indicates that the state will fully implement the concept or architectural guideline and be ready for the next steps.
- Verification (T/I/D) (Chapter 4 only) – the verification method assigned to this compatibility criterion by FMCSA for Core CVISN requirements
  - (T) Verify through interoperability testing
  - (I) Verify through inspection of documentation
  - (D) Verify with a less formal demonstration
- Comments – available for the state to explain "partial" or "no" commitment ratings
- Note: shaded cells in tables require no user entry

If the state maintains its master copy of this document electronically, the following conventions are recommended when filling in the columns to illustrate the "firmness" of the state's plan:

- *Italics font*: Tentative, not approved by the final decision makers
- Regular font: Approved by the decision makers (or supported by consensus)
- **Bold font**: Completed

States should fill in the “Commit Level” column for the tables in Chapter 2 (Guiding Principles), Chapter 3 (State Institutional Framework), and Chapter 4 (State Systems Checklists) during the CVISN program initiation phase. The remainder of the columns will be completed as the program progresses.

Appendix A, *Core CVISN Checklist*, enables states to easily correlate the Core CVISN requirements with interoperability tests and with check-off tests and demonstrations as they are completed. Instructions for using the checklist are provided in Appendix A.

2. GUIDING PRINCIPLES

Statements of guiding principles capture concepts and guidelines supported by the Commercial Vehicle Operations (CVO) community to provide a top-level checklist of fundamental guidelines for all CVISN activities. CVO stakeholders should ensure that their actions are consistent with these principles. No verification columns are included in the tables for guiding principles because the principles provide guidance rather than specific details that can be scheduled or measured.

The guiding principles were developed under the auspices of the Intelligent Transportation Systems (ITS) America CVO Program Subcommittee [References 7, 8, 9]. These principles are reviewed regularly by ITS America and the U.S. Department of Transportation (USDOT). They will be updated as required to reflect the consensus of the CVO community. *The current principles are copied verbatim into the tables in this chapter.*

2.1 ITS/CVO Guiding Principles

"The ITS America CVO Committee presents this set of guiding principles which will guide the states and federal government on matters concerning technology and commercial vehicle operations. This list of 39 guiding principles was established by the CVO Programs Subcommittee with representation from National Private Truck Council, ATA [American Trucking Associations], *carriers, owner operators, motorcoach representation, UPS* [United Parcel Service], *several state administrative and regulatory agencies, AAMVA* [American Association of Motor Vehicle Administrators], *AASHTO* [American Association of State Highway and Transportation Officials], *and Canada. These principles took two years to create and 100% consensus was reached."* [Reference 7]

2.1.1 ITS/CVO Guiding Principles: Summary

Table 2.1–1
ITS/CVO Guiding Principles: Summary

Commit Level (F/P/N)	Item #	ITS/CVO Guiding Principles: Summary Compatibility Criteria	Comments
	1.	A balanced approach involving ITS/CVO technology as well as institutional changes will be used to achieve measurable improvements in efficiency and effectiveness for carriers, drivers, governments, and other CVO stakeholders. Specific technology and process choices will be largely market-driven.	
	2.	The CVISN architecture will enable electronic information exchange among authorized stakeholders via open standards.	
	3.	The architecture deployment will evolve incrementally, starting with legacy systems where practical and proceeding in manageable steps with heavy end-user involvement.	
	4.	Safety assurance activities will focus resources on high risks, and be structured so as to reduce the compliance costs of low-risk carriers and drivers.	
	5.	Information technology will support improved practices and procedures to improve CVO credential and tax administration efficiency for carriers and government.	
	6.	Roadside operations will focus on eliminating unsafe and illegal operations by carriers, drivers, and vehicles without undue hindrance to productivity and efficiency of safe and legal carriers and drivers.	

Note: F – Full Commitment; P – Partial Commitment; N – No Commitment.
Complete code descriptions are given in Section 1.4.

2.1.2 ITS/CVO Guiding Principles: General CVO

Table 2.1–2
ITS/CVO Guiding Principles: General CVO

Commit Level (F/P/N)	Item #	ITS/CVO Guiding Principles: General CVO Compatibility Criteria	Comments
	1.	To the extent possible, ITS/CVO technology development and deployment will be market-driven. The federal role in ITS deployment will be limited to instances in which a government role is indispensable and in which the technology is proven and reliable.	
	2.	Investment and participation in ITS/CVO technology will be voluntary.	
	3.	The relative benefits of various ITS/CVO technology applications and investments will be assessed quantitatively using measures of effectiveness and established methods of quality control.	
	4.	Potential ITS/CVO technology applications will be evaluated against regulatory choices involving low-technology and non-technological options to ensure applications are cost-effective for both government and industry.	
	5.	Government CVO policies and regulatory practices will permit safe and legal carriers and drivers to operate without unnecessary regulatory and administrative burdens.	
	6.	Stakeholders will use technology and institutional reform to implement continuous process improvement and cost-effective process re-engineering.	
	7.	The confidentiality of proprietary and other sensitive stakeholder information will be preserved.	
	8.	The United States CVO community will work to implement compatible policies and architecture and interoperable systems in all states.	

Commit Level (F/P/N)	Item #	ITS/CVO Guiding Principles: General CVO Compatibility Criteria	Comments
	9.	The United States CVO community will work with those in Canada, Mexico, and other nations to encourage compatible policies and architecture and to implement interoperable systems throughout North America and, when possible, worldwide.	

Note: F – Full Commitment; P – Partial Commitment; N – No Commitment.
Complete code descriptions are given in Section 1.4.

2.1.3 ITS/CVO Guiding Principles: CVISN Architecture

Table 2.1–3
ITS/CVO Guiding Principles: CVISN Architecture

Commit Level (F/P/N)	Item #	ITS/CVO Guiding Principles: CVISN Architecture Compatibility Criteria	Comments
	1.	The CVISN architecture will be open, modular, and adaptable.	
	2.	The architecture will enable data exchange among systems, a key to reaching CVO objectives. Methods used to exchange data will ensure data integrity and prevent unauthorized access.	
	3.	Data exchange will be achieved primarily via common data definitions, message formats, and communication protocols. These enable development of interoperable systems by independent parties.	
	4.	A jurisdiction shall have and maintain ownership of any data collected by any agent on its behalf.	
	5.	The architecture will accommodate existing and near-term communications technologies.	
	6.	The architecture will accommodate proven technologies and legacy systems whenever possible.	
	7.	The CVISN architecture will allow government and industry a broad range of options, open to competitive markets, in CVO technologies.	

Note: F – Full Commitment; P – Partial Commitment; N – No Commitment.
Complete code descriptions are given in Section 1.4.

2.1.4 ITS/CVO Guiding Principles: CVISN Deployment

Table 2.1–4
ITS/CVO Guiding Principles: CVISN Deployment

Commit Level (F/P/N)	Item #	ITS/CVO Guiding Principles: CVISN Deployment Compatibility Criteria	Comments
	1.	The feasibility of the architecture will be demonstrated incrementally in simulations, prototypes, operational tests, and pilots. There will be heavy end-user involvement in each step of the process.	
	2.	After feasibility has been demonstrated, key architectural elements will be incorporated into appropriate national and international standards.	
	3.	The architecture deployment will evolve incrementally, starting with legacy systems where practical and proceeding in manageable steps.	
	4.	Strong federal leadership will foster voluntary cooperative efforts within government jurisdictions and among groups of other stakeholders to develop systems which are in accord with the architecture.	

Note: F – Full Commitment; P – Partial Commitment; N – No Commitment.
Complete code descriptions are given in Section 1.4.

2.1.5 ITS/CVO Guiding Principles: Safety Assurance

Table 2.1–5
ITS/CVO Guiding Principles: Safety Assurance

Commit Level (F/P/N)	Item #	ITS/CVO Guiding Principles: Safety Assurance Compatibility Criteria	Comments
	1.	Carriers and drivers will be responsible for the safe and legal operation of commercial vehicles.	
	2.	Jurisdictions will develop and implement uniform standards, practices, procedures, and education programs to improve safety. These activities will leverage market forces that encourage safety.	
	3.	Jurisdictions will focus safety enforcement resources on high risk carriers and drivers. They will remove chronic poor performers from operation and help cooperative marginal performers to improve.	
	4.	Jurisdictions will conduct inspections and audits to provide incentives for carriers and drivers to improve poor performance and to collect information for assessing carrier and driver performance.	
	5.	Jurisdictions will use a safety risk rating for all carriers based on best available information and common criteria.	
	6.	Jurisdictions will identify high risk drivers based on best available information and common criteria.	
	7.	Safety programs will provide benefits which exceed costs for carriers and drivers as well as governments.	

Note: F – Full Commitment; P – Partial Commitment; N – No Commitment.
Complete code descriptions are given in Section 1.4.

2.1.6 ITS/CVO Guiding Principles: Credentials & Tax

Table 2.1–6
ITS/CVO Guiding Principles: Credentials & Tax

Commit Level (F/P/N)	Item #	ITS/CVO Guiding Principles: Credentials & Tax Compatibility Criteria	Comments
	1.	Electronic information will be used in place of paper documents for the administration of CVO credential and tax requirements.	
	2.	Authorized users will be able to electronically exchange credential and tax-related information and funds via open standards and transmission options.	
	3.	The information needed to administer tax and credential programs involving carriers, drivers, and vehicles will be available to authorized officials, on a need-to-know basis.	
	4.	Individual jurisdictions, or their designated agent, will be the authoritative source of information on credentials they issue.	

Note: F – Full Commitment; P – Partial Commitment; N – No Commitment.
Complete code descriptions are given in Section 1.4.

2.1.7 ITS/CVO Guiding Principles: Roadside Operations

Table 2.1–7
ITS/CVO Guiding Principles: Roadside Operations

Commit Level (F/P/N)	Item #	ITS/CVO Guiding Principles: Roadside Operations Compatibility Criteria	Comments
	1.	Roadside operations will focus on eliminating unsafe and illegal operations by carriers, drivers, and vehicles and will be designed and administered to accomplish this in a manner that does not unduly hinder the productivity and efficiency of safe and legal motor carriers and drivers.	
	2.	Jurisdictions will support CVO roadside operations programs with timely, current, accurate, and verifiable electronic information, making it unnecessary for properly equipped vehicles to carry paper credentials.	

Note: F – Full Commitment; P – Partial Commitment; N – No Commitment.
Complete code descriptions are given in Section 1.4.

2.2 Fair Information Principles (FIP) for ITS/CVO

"These fair information principles were prepared in recognition of the importance of protecting individual privacy in implementing Intelligent Transportation Systems (ITS) for Commercial Vehicle Operations (CVO). They have been adopted by the ITS America CVO Technical Committee.

These principles represent values and are designed to be flexible and durable to accommodate a broad scope of technological, social, and cultural change. ITS America may, however, need to revisit them periodically to assure their applicability and effectiveness.

These principles are advisory, intended to educate and guide transportation professionals, policy-makers, and the public as they develop fair information and privacy guidelines for specific ITS/CVO projects. They are not intended to supersede existing statutes or regulations. Initiators of ITS/CVO projects are urged to publish the fair information principles that they intend to follow. Parties to ITS/CVO projects are urged to include enforceable provisions for safeguarding privacy in their contracts and agreements". [Reference 8]

Table 2.2–1
Fair Information Principles for ITS/CVO

Commit Level (F/P/N)	Item #	Fair Information Principles for ITS/CVO Compatibility Criteria	Comments
	FIP #1	***Privacy*** The reasonable expectation of privacy regarding access to and use of personal information should be assured. The parties must be reasonable in collecting data and protecting the confidentiality of that data.	
	FIP #2	***Integrity*** Information should be protected from improper alteration or improper destruction.	
	FIP #3	***Quality*** Information shall be accurate, up-to-date, and relevant for the purposes for which it is provided and used.	
	FIP #4	***Minimization*** Only the minimum amount of relevant information necessary for ITS applications shall be collected; data shall be retained for the minimum possible amount of time.	
	FIP #5	***Accountability*** Access to data shall be controlled and tracked; civil and criminal sanctions should be imposed for improper access, manipulation, or disclosure, as well as for knowledge of such actions by others.	
	FIP #6	***Visibility*** There shall be disclosure to the information providers of what data are being collected, how they are collected, who has access to the data, and how the data will be used.	
	FIP #7	***Anonymity*** Data shall not be collected with individual driver identifying information, to the extent possible.	
	FIP #8	***Design*** Security should be designed into systems from the beginning, at a system architecture level.	

Commit Level (F/P/N)	Item #	Fair Information Principles for ITS/CVO Compatibility Criteria	Comments
	FIP #9	***Technology*** Data encryption and other security technologies shall be used to make data worthless to unauthorized users.	
	FIP #10	***Use*** Data collected through ITS applications should be used only for the purposes that were publicly disclosed.	
	FIP #11	***Secondary Use*** Data collected by the private sector for its own purposes through a voluntary investment in technology should not be used for enforcement purposes without the carrier's consent.	

Note: F – Full Commitment; P – Partial Commitment; N – No Commitment.
Complete code descriptions are given in Section 1.4.
Date approved by the Board of Directors: April 22, 1999.

Note: These guiding principles address only issues of privacy and data control. They do not address all issues related to concepts of operations or interoperability. These issues are addressed in separate guiding principles.

2.3 ITS/CVO Interoperability Guiding Principles (IGP)

"These interoperability guiding principles were prepared in recognition of the importance of promoting interoperability in the implementation of Intelligent Transportation Systems (ITS) for Commercial Vehicle Operations (CVO). They have been adopted by the ITS America CVO Technical Committee.

These principles represent values and are designed to be flexible and durable to accommodate a broad scope of technological, social, and cultural change. ITS America may, however, need to revisit them periodically to assure their applicability and effectiveness.

These principles are advisory, intended to educate and guide transportation professionals, policy-makers, and the public as they develop interoperability guidelines for specific ITS/CVO projects. They are not intended to supersede existing statutes or regulations. Initiators of ITS/CVO projects are urged to publish the interoperability principles that they intend to follow. Parties to ITS/CVO projects are urged to include enforceable provisions for assuring interoperability in their contracts and agreements." [Reference 9]

2.3.1 ITS/CVO Interoperability Guiding Principles: General

Table 2.3–1
ITS/CVO Interoperability Guiding Principles: General

Commit Level (F/P/N)	Item #	ITS/CVO Interoperability Guiding Principles: General Compatibility Criteria	Comments
	IGP #1	The CVO community will work to implement interoperable ITS/CVO systems in all United States jurisdictions.	
	IGP #2	The CVO community will work with the CVO communities in Canada and Mexico to implement interoperable ITS/CVO systems throughout North America.	
	IGP #3	The CVO community will work to ensure that ITS/CVO systems, where appropriate, are interoperable with other ITS systems (e.g., electronic toll systems).	
	IGP #4	Interoperable ITS/CVO systems will be achieved through the development, adoption, and adherence to common standards for hardware, systems/software, operations, and program administration.	
	IGP #5	Each jurisdiction will support the national ITS/CVO information system architecture and data exchange standards developed under the Commercial Vehicle Information Systems and Networks (CVISN) program.	
	IGP #6	Transponders shall have a unique identifier.	
	IGP #7	Information systems supporting electronic screening, credentials administration, and safety assurance will use: 7a. USDOT numbers for the identification of both interstate and intrastate motor carriers. 7b. Commercial Drivers License (CDL) numbers for the identification of commercial drivers. 7c. Vehicle Identification Numbers (VIN) and license plate numbers for the identification of power units.	

Note: F – Full Commitment; P – Partial Commitment; N – No Commitment.
Complete code descriptions are given in Section 1.4.

2.3.2 ITS/CVO Interoperability Guiding Principles: Hardware

Table 2.3–2
ITS/CVO Interoperability Guiding Principles: Hardware

Commit Level (F/P/N)	Item #	ITS/CVO Interoperability Guiding Principles: Hardware Compatibility Criteria	Comments
	IGP #8	Commercial vehicle operators will be able to use one transponder for power unit-to-roadside communications in support of multiple applications including electronic screening, safety assurance, fleet and asset management, tolls, parking, and other transaction processes.	
	IGP #9	Public and public-private Dedicated Short Range Communications (DSRC) applications will support open standards that are consistent with the national ITS architecture.	

Note: F – Full Commitment; P – Partial Commitment; N – No Commitment.
Complete code descriptions are given in Section 1.4.

2.3.3 ITS/CVO Interoperability Guiding Principles: Systems/Software

Table 2.3–3
ITS/CVO Interoperability Guiding Principles: Systems/Software

Commit Level (F/P/N)	Item #	ITS/CVO Interoperability Guiding Principles: Systems/Software Compatibility Criteria	Comments
	IGP #10	Public and public-private organizations will support open data exchange standards for the state-state, state-federal, state-provincial, and carrier-agency exchange of safety and credentials information as described in the national ITS architecture.	

Note: F – Full Commitment; P – Partial Commitment; N – No Commitment.
Complete code descriptions are given in Section 1.4.

2.3.4 ITS/CVO Interoperability Guiding Principles: Operations

Table 2.3–4
ITS/CVO Interoperability Guiding Principles: Operations

Commit Level (F/P/N)	Item #	ITS/CVO Interoperability Guiding Principles: Operations Compatibility Criteria	Comments
	IGP #11	Jurisdictions will support common standards for placement of DSRC transponders on trucks and buses to ensure the safe and cost-effective use of transponders.	
	IGP #12	Jurisdictions will support a common set of recommended practices concerning the selection, layout, and signage of roadside screening sites (i.e., weigh stations, ports-of-entry, international border crossings, and temporary inspection sites) to ensure safe operations.	
	IGP #13	Jurisdictions will support a common performance standard for roadside electronic enforcement screening and passage of transponder-equipped motor carriers to ensure equity in enforcement.	
	IGP #14	Roadside electronic enforcement screening criteria will include the following: motor carriers must be enrolled in the jurisdiction's program; must meet the jurisdiction's enrollment criteria; and must meet all legal requirements established by the jurisdiction.	
	IGP #15	Jurisdictions will support quarterly reviews of carrier qualifications to ensure that the standards evolve to meet the changing needs of government and motor carriers.	
	IGP #16	A jurisdiction will not retain the identification codes or other data from the DSRC transponders of passing motor carriers who are not enrolled in the jurisdiction's program.	
	IGP #17	Jurisdictions will support a common performance standard for selection of vehicles and drivers for roadside safety inspection.	
	IGP #18	Jurisdictions will support a common performance standard for recording and reporting roadside safety inspection results.	
	IGP #19	Jurisdictions will support a common performance standard for reconciling disputed roadside safety inspection results.	

Note: F – Full Commitment; P – Partial Commitment; N – No Commitment.
Complete code descriptions are given in Section 1.4.

2.3.5 ITS/CVO Interoperability Guiding Principles: Program

Table 2.3–5
ITS/CVO Interoperability Guiding Principles: Program

Commit Level (F/P/N)	Item #	ITS/CVO Interoperability Guiding Principles: Program Compatibility Criteria	Comments
	IGP #20	Motor carrier participation in ITS/CVO roadside electronic screening programs will be voluntary; motor carriers will not be required to purchase or operate DSRC transponders.	
	IGP #21	Motor carriers will have the option of enrolling in any ITS/CVO roadside electronic screening program.	
	IGP #22	Jurisdictions will support uniform criteria for enrollment of motor carriers in ITS/CVO roadside screening programs.	
	IGP #23	Enrollment criteria will include consideration of safety performance and credentials status (e.g., registration, fuel and highway use taxes, and insurance).	
	IGP #24	No jurisdiction will be required to enroll motor carriers that do not meet the criteria for enrollment.	
	IGP #25	Motor carriers may obtain a DSRC transponder from the enrolling jurisdiction or a compatible DSRC transponder from an independent equipment vendor of the motor carrier's choice.	
	IGP #26	Each jurisdiction will determine the price and payment procedures, if any, for motor carriers to enroll and participate in its ITS/CVO electronic screening program.	
	IGP #27	Jurisdictions shall work to establish business interoperability agreements among roadside electronic screening programs.	
	IGP #28	A jurisdiction will make a motor carrier's DSRC transponder unique identifier available to another jurisdiction upon written request and authorization by the motor carrier.	

Commit Level (F/P/N)	Item #	ITS/CVO Interoperability Guiding Principles: Program Compatibility Criteria	Comments
	IGP #29	Jurisdictions will work toward development of a single point of contact for motor carriers enrolling in more than one ITS/CVO roadside screening program.	
	IGP #30	Each jurisdiction will fully disclose and publish its practices and policies governing, at a minimum: 30a. Enrollment criteria; 30b. Transponder unique identifier standards; 30c. Price and payment procedures for transponders and services; 30d. Screening standards; 30e. Use of screening event data; and 30f. Business interoperability agreements with other programs.	

Note: F – Full Commitment; P – Partial Commitment; N – No Commitment.
Complete code descriptions are given in Section 1.4.
Date approved by the Board of Directors: April 22, 1999.

Note: These guiding principles address only issues of interoperability. They do not address all issues related to concepts of operations or privacy and data control. These issues are addressed in separate guiding principles.

3. STATE INSTITUTIONAL FRAMEWORK

The checklist in this section summarizes the institutional and business planning steps that states should take to become ready to implement the CVISN Architecture and concepts. The checklist is based on the ideas outlined in the *CVISN Model Deployment Initiative* in the late 1990s.

Table 2.3–1
State Institutional Framework

Commit Level (F/P/N)	Item #	State Institutional Framework Compatibility Criteria	Comments
	1.	The state has contacted or has plans to contact state and local transportation officials to explore potential joint-uses of transponders and ensure integration among multiple applications (i.e., CVO, toll, traffic probes, parking management, etc.)	
	2.	The state has evaluated or has plans to evaluate the data that is being collected for CVISN initiatives to determine if other state and local transportation entities (e.g., traffic management center) outside the CVO community could use the data, which is collected under CVISN deployment, consistent with data privacy agreements.	
	3.	The state has conducted or has plans to conduct outreach to its motor carrier partners about metropolitan and rural ITS initiatives within the state that could provide benefits to its motor carrier operations. Examples of these initiatives include Web sites on roadway weather information systems, incident management systems, and traffic management systems.	
	4.	The state is committed to complete training as appropriate, and upon completion, to begin deployment of the ITS/CVO systems and services that meet the unique economic, administrative, and transportation needs, as outlined in the state ITS/CVO Business Plan.	

Commit Level (F/P/N)	Item #	State Institutional Framework Compatibility Criteria	Comments
	5.	A qualified core project team has been identified. This project team must include the following individuals: the state's CVISN project manager; the state's CVISN system architect; a project facilitator/administrator, who could be a representative of a participating state agency or a consultant working with the state; operations staff representing the agencies responsible for the state's major CVO functional areas [i.e., International Registration Plan (IRP), International Fuel Tax Agreement (IFTA), safety information systems, roadside safety inspections, size and weight enforcement, and credentials enforcement]; staff from the state department of information technology or comparable information technology units within the state CVO agencies; representative of the state Department of Transportation; representatives of the FMCSA and Federal Highway Administration (FHWA) Division office; and a motor carrier industry representative (invited).	
	6.	Appropriate and sufficient staff, equipment, and state and private funding are available to carry out the deployment of CVISN and ITS/CVO services. The CVISN project has sufficient priority (i.e., other higher-priority projects are not competing for the same resources).	
	7.	A state CVO strategic plan and/or business plan exists and has been accepted by the FHWA (or FMCSA). It outlines the goals, strategies, anticipated benefits and costs, organization, projects, schedules, and resources relevant to achieving the envisioned CVO environment.	
	8.	A planning and coordination process exists which includes all state agencies involved in any aspect of motor carrier safety and regulation.	
	9.	The top executives and chief information systems managers of each involved agency have endorsed state CVO plans and given the CVISN project manager adequate authority.	
	10.	A process for resolution of conflicts among participating agencies exists.	
	11.	State agencies have a strong commitment to customer service and the ability to work with the motor carrier industry in their state.	
	12.	State agencies involve the motor carrier industry in the planning process.	
	13.	State agencies conduct education programs to improve the safety performance and regulatory compliance of motor carriers.	

Commit Level (F/P/N)	Item #	State Institutional Framework Compatibility Criteria	Comments
	14.	State agencies provide periodic forums for obtaining suggestions and concerns from the motor carrier industry.	
	15.	State agencies actively pursue opportunities for and implement business process reengineering projects.	
	16.	An e-mail system is available among agencies.	
	17.	At least key agency staff members have access to the Internet.	
	~~18.~~	~~The state has adopted an open standard [American National Standards Institute Accredited Standards Committee (ANSI ASC) X12, for example] for EDI with the public.~~	Requirement deleted.
	19.	The state's communications infrastructure is sufficiently developed to extend to the kinds of electronic data exchanges needed under the CVISN Architecture.	
	20.	There are no state legislative barriers relative to data privacy, physical signature requirements, data exchange among agencies, data exchange with other states, or other uses of information technology required to implement the CVISN concept of operations.	
	21.	The legislature provides adequate resources to support an active ITS/CVO program and deployment of the ITS/CVO services.	
	22.	The state participates in one or more regional CVO forums to assist in developing regional and national interoperable systems and compatible policies and procedures. The state participates in CVO discussions with other CVISN states.	
	23.	The state is willing to provide timely, electronic information to the IRP and IFTA clearinghouses to support the base jurisdictions agreements.	
	24.	The project team has completed the ITS/CVO technical training courses or equivalent.	
	25.	*Requirement deleted in previous version of this document.*	
	26.	Effective procurement plans and processes are in place to acquire services and equipment needed to support the CVISN project, and the CVISN team is aware of constraints the processes impose.	
	27.	Effective subcontract management processes are in place and allow timely identification and resolution of performance problems.	

Commit Level (F/P/N)	Item #	State Institutional Framework Compatibility Criteria	Comments
	28.	The CVISN team has a clear understanding of the state-specific requirements for information technology projects, e.g., whether or not a feasibility study is required.	
	29.	The CVISN team has a clear understanding of the state-specific budget cycles and is aware of constraints they impose.	

Note: F – Full Commitment; P – Partial Commitment; N – No Commitment.
Complete code descriptions are given in Section 1.4.

4. STATE SYSTEMS CHECKLISTS

The checklists in this chapter describe operational concepts and state systems design requirements. The checklists are divided into these categories:

- Section 4.1 General Operational Concepts and State Systems Design Requirements
- Section 4.2 State Safety Information Exchange and Safety Assurance Operational Concepts and Systems Design Requirements
- Section 4.3 State Commercial Vehicle (CV) Administration Operational Concepts and Systems Design Requirements
- Section 4.4 State Electronic Screening Operational Concepts and Systems Design Requirements

Operational concepts and state systems design requirements in Section 4.1 “General Operational Concepts and State Systems Design Requirements” apply to Sections 4.2, 4.3, and 4.4.

For each category there are two tables.

- The first table in each category lists Operational Concepts. The concepts are based on an interpretation of the guiding principles and the state of existing and emerging technologies. The guiding principles and operational concepts led to the system design requirements. The operational concepts are not testable.
- The second table in each category lists top-level requirements for the design of state systems. The tables show more detail about what “Core CVISN” means. The Core CVISN requirements are marked with “Core” in the fourth column [Req Level (Core/Expanded)]. The approach for verifying the Core CVISN requirements is identified in the Verification column. “T” means interoperability tests are used to verify the item. “I” means verification by inspection of documentation. “D” means verification by less formal demonstration. If a cell is blank, then no verification method has been specified.

Note: shaded cells in these tables require no user entry.

4.1 General Operational Concepts and State Systems Design Requirements

The general operational concepts and state systems design requirements apply to **all** state systems. They facilitate interoperability and the exchange of information within a single state and across jurisdictions. These requirements apply to safety, credentialing, and electronic screening systems.

FMCSA's policy on electronic credentials administration between motor carriers and states is:

- FMCSA requires that states implement either a person-to-computer or a computer-to-computer interface.
- FMCSA recommends that states survey their stakeholders to determine whether both interfaces would be appropriate.

This is a policy regarding Core CVISN. If a state chooses to first implement a Web-based (person-to-computer) credentialing approach, then implementation of a computer-to-computer interface is considered an Expanded CVISN capability. Similarly, if a state first chooses to implement a computer-to-computer credentialing approach, then implementation of a Web-based interface is considered an Expanded CVISN capability.

The concepts in Table 4.1–1 are based on an interpretation of the guiding principles and existing and emerging technologies. The guiding principles and operational concepts led to the system design requirements. The operational concepts are not testable.

Table 4.1–1
General Operational Concepts

Commit Level (F/P/N)	Item #	General Operational Concepts Compatibility Criteria	Req Level (Core/ Expanded)	Comments
	1.	Good business processes can be enhanced through improved automated access to accurate information.	Core	
	2.	Authoritative sources are responsible for maintaining accurate information. Each jurisdiction participating in ITS/CVO information exchange identifies the authoritative source for each data item. Sometimes authoritative systems authorize indirect sources to assist in the information exchange process.	Core	
	3.	Subsumed by #2 above.		
	4.	To enable cross-referencing and standard look-ups in multiple information systems, a common scheme for identifying carriers must be adopted. The Primary Carrier ID should be used in interface agreements (open standards, Internet-based exchanges, and custom interface agreements) to facilitate the exchange of carrier information. How the ID is stored internally outside the interface is up to the system implementers.	Core	
	a.	The ID should be based on the USDOT number for interstate carriers.	Core	
	b.	The Primary Carrier ID should be based on the USDOT number for intrastate carriers. If the state does not use the USDOT number as the ID for its intrastate carriers, then the state should establish a Primary Carrier ID for each intrastate carrier in that state.	Core; Expanded – based on USDOT number	

Commit Level (F/P/N)	Item #	General Operational Concepts Compatibility Criteria	Req Level (Core/ Expanded)	Comments
	5.	To enable cross-referencing and standard look-ups in multiple information systems, a common scheme for identifying drivers must be adopted for interstate and intrastate operators. The CDL number should be the basis of the Driver ID.	Core	
	6.	To enable cross-referencing and standard look-ups in multiple information systems, a common scheme for identifying vehicles must be adopted for interstate and intrastate operators. The VIN and jurisdiction plus license plate numbers should be the bases for the identification of power units.	Core	
	7.	To enable cross-referencing and standard look-ups in multiple information systems, a common scheme for identifying international trips must be adopted. The Trip/Load number consisting of Data Universal Numbering System (DUNS) and trip-specific ID should be the basis for identifying international trips.	Expanded	
	8.	Standard information exchange is supported via carrier and vehicle (and eventually driver) snapshots.	Core – carrier and vehicle; Expanded – driver	
	9.	Flexible implementation/deployment options are accommodated by the ITS/CVO architecture. As technology changes, so will the architecture.	Core	
	10.	Open standards are used for interchanges between public and private computer systems. (HTML/XML are used for most carrier-state information systems' interactions. DSRC standards for the messages, data link, and physical layers are used for vehicle-roadside interactions.)	Core	

Commit Level (F/P/N)	Item #	General Operational Concepts Compatibility Criteria	Req Level (Core/ Expanded)	Comments
	11.	Electronic data exchange will allow all activities to focus resources on high risk operators.	Core	
	12.	Interoperability is assured by executing standardized interoperability tests. If a tested system is changed, the interoperability tests are re-run as part of the re-validation process.	Core	
	13.	The Fair Information Principles for ITS/CVO will be implemented using a combination of policies, procedures, technology, and training. Stakeholders will be included in the discussions of the techniques to be used to implement the principles.	Core	
	14.	Citations are based on a review of real-time conditions and checks with authoritative sources.	Core	
	15.	The Internet is used as a wide area network for information exchange.	Core	
	16.	The World Wide Web is used for interactions and information exchanges between private people and government systems (e.g., for credentials applications or commercial vehicle regulations).	Core	
	17.	The CVISN Program is structured to encourage focus on sharing data among safety, credentialing and screening processes. States are encouraged to design and deploy these three elements in parallel.	Core	

Note: F – Full Commitment; P – Partial Commitment; N – No Commitment
Core – Core CVISN; Expanded – Expanded CVISN capability
Complete code descriptions are given in Section 1.4.

The Core CVISN general state systems design requirements can be summarized as follows:

- An organizational framework for cooperative system development has been established among state agencies and motor carriers.
- A state CVISN System Design has been established that conforms to the CVISN Architecture and can evolve to include new technology and capabilities.
- All the elements of three capability areas (Safety Information Exchange, Credentials Administration, and Electronic Screening, described in Sections 4.2, 4.3, and 4.4, respectively) have been implemented using applicable architectural guidelines, operational concepts, and standards.

The state systems requirements in Table 4.1–2 apply to the design of all state systems. The table shows more detail about what "Core CVISN" means. The Core CVISN requirements are marked with "Core" in the fourth column [Req Level (Core/Expanded)]. The Verification column only applies to Core CVISN requirements. For an overview of Core CVISN, see the *Introductory Guide to CVISN* [Reference 2].

Table 4.1–2
General State Systems Design Requirements Checklist

Commit Level (F/P/N)	Item #	General State Systems Design Requirements Checklist Compatibility Criteria	Req Level (Core/ Expanded)	Verification (T/I/D)	Comments
	4.1.1	Adopt standard identifiers for carriers, vehicles, drivers, and transponders to support information exchange.	Core	T	
	1	Adopt standard identifiers for interstate carrier, vehicle, driver, and transponder.	Core	T	
	2	Adopt standard identifiers for intrastate carrier, vehicle, driver, and transponder.	Expanded		
	4.1.2	Use the World Wide Web for person-to-computer interactions between private citizens and state information systems.	Core	T	
	4.1.3	Use open standards for computer-to-computer exchange of information with other jurisdictions and with the public.	Core	T	
	1	Use open standards[1] for transactions between state information systems and private systems [Commercial Vehicle (CV) operators, insurance companies, etc.].	Core	T	
	2	Use open standards for transactions between state information systems and CVISN Core Infrastructure systems, where available.	Core	T	
	3	Use XML standards for transactions between state information systems and private systems (CV operators, insurance companies, etc.).	Expanded		

[1] Open standards are publicly available specifications or standards that promote interoperability.

Commit Level (F/P/N)	Item #	General State Systems Design Requirements Checklist Compatibility Criteria	Req Level (Core/ Expanded)	Verification (T/I/D)	Comments
	4.1.4	Ensure that all information transfers, fee payments, and money transfers are authorized and secure, e.g., through access control and encryption.	Core	D	
	4.1.5	Exchange safety and credentials data electronically within the state to support credentialing, safety, and other roadside functions. Where useful, exchange snapshots.	Core	T	
	1	Data for interstate carriers	Core	T	
	2	Data for interstate vehicles	Core	T	
	3	Data for intrastate carriers	Core	D	
	4	Data for intrastate vehicles	Core	D	
	5	Data for drivers	Expanded		
	4.1.6	Demonstrate technical interoperability by performing Interoperability Tests.	Core	D	
	4.1.7	Support electronic payments.	Expanded		
	4.1.8	Receive, collect, and archive relevant CVO data for historical, secondary, and non-real-time uses.	Expanded		

Note: F – Full Commitment; P – Partial Commitment; N – No Commitment
Core – Core CVISN; Expanded – Expanded CVISN capability
T – interoperability Testing; I – Inspection of documentation; D – Demonstration
Complete code descriptions are given in Section 1.4.

4.2 State Safety Information Exchange and Safety Assurance Operational Concepts and Systems Design Requirements

The state safety information exchange and safety assurance systems are likely to consist of:

- Inspection (e.g., ASPEN)
- SAFETYNET
- Citation & Accident
- Compliance Review [e.g., Compliance Analysis Performance Review Information (CAPRI)]
- Commercial Vehicle Information Exchange Window (CVIEW) or equivalent

The state CV safety information exchange and safety assurance systems will operate at one or more locations within a state. The systems perform safety information exchange and safety assurance functions supporting safety regulations. States may form regional alliances to support these functions. Each state coordinates with other states, regional alliances, and CVISN Core Infrastructure systems to support nationwide access to safety information for administrative and enforcement functions.

The concepts in Table 4.2–1 are based on an interpretation of the guiding principles and existing and emerging technologies. The guiding principles and operational concepts led to the system design requirements. The operational concepts are not testable.

Table 4.2–1
Safety Information Exchange and Safety Assurance Operational Concepts

Commit Level (F/P/N)	Item #	Safety Information Exchange and Safety Assurance Operational Concepts Compatibility Criteria	Req Level (Core/ Expanded)	Comments
	1.	Data are collected electronically to improve roadside safety enforcement activities.	Core	
	2.	Electronic safety records (snapshots) are made available at the roadside to aid inspectors and other enforcement personnel.	Core	
	3.	Inspectors use computer applications to capture, verify, and submit intrastate and interstate inspection data at the point of inspection.	Core	
	4.	Safety data are made available electronically to qualified stakeholders in accordance with privacy agreements.	Core	
	5.	User access to data is controlled (restricted and/or monitored) where necessary.	Core	
	6.	Mechanisms are made available for operators to dispute safety records held by government systems.	Core	
	7.	Compliance reviews are supported through electronic access to government-held safety records.	Expanded	
	8.	Safety risk ratings are determined according to uniform guidelines.	Expanded	
	9.	Jurisdictions support a standard set of criteria for inspection selection.	Expanded	
	10.	A comprehensive safety policy, including roadside and deskside activities, is implemented to improve safety.	Expanded	
	11.	Carriers are associated with a base state for safety information record storage and credentialing.	Expanded	
	12.	Compliance reviews are supported through electronic access to carrier-held records.	Expanded	

Note: F – Full Commitment; P – Partial Commitment; N – No Commitment
Core – Core CVISN; Expanded – Expanded CVISN capability
Complete code descriptions are given in Section 1.4.

Core CVISN state safety information exchange and safety assurance systems design requirements can be summarized as follows:

- Inspection reporting using ASPEN (or equivalent) at all major inspection sites. ASPEN data sent to Safety and Fitness Electronic Records (SAFER) directly or indirectly.
- Connection to SAFER system to provide exchange of interstate carrier and vehicle data snapshots among states.
- Implementation of the CVIEW (or equivalent) system for exchange of intrastate and interstate data within state and connection to SAFER for exchange of interstate data through snapshots.

– OR –

- Utilization of SAFER option for exchange of inter- and intrastate data through snapshots.

The state systems requirements in Table 4.2–2 apply to the design of state safety-related systems. The table shows more detail about what "Core CVISN" means. The Core CVISN requirements are marked with "Core" in the fourth column [Req Level (Core/Expanded)]. For an overview of Core CVISN, see the *Introductory Guide to CVISN* [Reference 2].

Table 4.2–2
State Safety Information Exchange and Safety Assurance Systems Design Requirements Checklist

Commit Level (F/P/N)	Item #	State Safety Information Exchange and Safety Assurance Systems Design Requirements Checklist Compatibility Criteria	Req Level (Core/ Expanded)	Verification (T/I/D)	Comments
	4.2.1	Use ASPEN (or equivalent) at all major inspection sites	Core	D	
	1	Select vehicles and drivers for inspection based on availability of inspector, standard inspection selection system, vehicle measures, and random process, as statutes permit.	Core	D	
	2	Report interstate inspections to Motor Carrier Management Information System (MCMIS) via SAFETYNET.	Core	D	
	3	Report intrastate inspections to SAFETYNET.	Core	D	
	4	Submit interstate and intrastate inspections for temporary storage to SAFER.	Core	T/D	
	5	Periodically check Out-Of-Service (OOS) orders issued in the state to focus enforcement and safety assurance activities.	Expanded		
	6	To assist in inspection, use DSRC or other available technologies to retrieve summary vehicle safety sensor data, if driver allows and vehicle is properly equipped.	Expanded		
	7	To assist in inspection, use DSRC or other available technologies to retrieve driver's daily log, if driver allows and vehicle is properly equipped.	Expanded		
	8	Use electronically-generated driver's daily log, if driver offers, as an alternative to a manually-maintained log during an inspection.	Expanded		

Commit Level (F/P/N)	Item #	State Safety Information Exchange and Safety Assurance Systems Design Requirements Checklist Compatibility Criteria	Req Level (Core/ Expanded)	Verification (T/I/D)	Comments
	4.2.2	SAFETYNET submits inspection reports to SAFER.	Core	D	
	1	SAFETYNET submits interstate inspection reports to SAFER.	Core	D	
	2	SAFETYNET submits intrastate inspection reports to SAFER.	Core	D	
	4.2.3	Maintain snapshots (or equivalent information) for operators based in the state and make available to within-state information systems and authorized users.	Expanded		
	1	For any given snapshot, there is only one authoritative source (or group of authoritative sources, such as ASPEN units) for each field in that snapshot.	Expanded		
	2	Allow only the authoritative source to update a snapshot data field, with the following exception: • A "super user" can update any field. An audit trail should be maintained to record super user updates.	Expanded		
	3	Validate the data source through some industry-standard means [account ID, Internet Protocol (IP) address, password, security keys, ...].	Expanded		
	4	Reject updates attempted by any system other than the authoritative source or a super user with a code explaining why. The rejection transaction should be returned to the sender in a timely fashion. The rejection should be logged for the snapshot system administrator to review.	Expanded		
	4.2.4	Use CAPRI (or equivalent) for compliance reviews.	Core	D	
	1	Report interstate compliance reviews to MCMIS via SAFETYNET.	Core	D	
	4.2.5	Collect, store, analyze, and distribute citation data electronically.	Expanded		

Commit Level (F/P/N)	Item #	State Safety Information Exchange and Safety Assurance Systems Design Requirements Checklist Compatibility Criteria	Req Level (Core/ Expanded)	Verification (T/I/D)	Comments
	1	Report citations for interstate operators to MCMIS via SAFETYNET.	Expanded		
	4.2.6	Collect, store, analyze, and distribute crash data electronically.	Expanded		
	1	Report interstate crashes as required to MCMIS via SAFETYNET.	Expanded		
	4.2.7	Compute carrier safety risk rating for intrastate carriers based on safety data collected.	Expanded		
	4.2.8	Identify high risk drivers based in the state through regular performance evaluation of various factors such as license status, points, and inspections.	Expanded		
	4.2.9	Implement the CVIEW (or equivalent) system for exchange of intrastate and interstate data within state and connection to SAFER for exchange of interstate data through snapshots – OR – utilize the SAFER option for exchange of inter- and intrastate data through snapshots.	Core	T	
	1	Implement a state CVIEW.	Core	T	
	2	Implement a CVIEW equivalent system.	Core	T	
	3	Utilize the SAFER option.	Core	T	

Note: F – Full Commitment; P – Partial Commitment; N – No Commitment
Core – Core CVISN; Expanded – Expanded CVISN capability
T – interoperability Testing; I – Inspection of documentation; D – Demonstration
Complete code descriptions are given in Section 1.4.

4.3 State Commercial Vehicle (CV) Administration Operational Concepts and Systems Design Requirements

The state CV administration systems are likely to consist of:

- Interstate and Intrastate Vehicle Registration
- Fuel Tax Credentialing/Tax Return Processing
- Credentialing Interface
- Web site
- Carrier Registration
- Driver Licensing
- Titling
- Treasury or Revenue
- Hazardous Materials (HazMat) Credentialing/Permitting
- Oversize/Overweight (OS/OW) Permitting
- Electronic Screening Enrollment (ESE) – see Section 4.4 on Electronic Screening

These systems operate at one or more (generally) fixed locations within a state. The systems perform administrative functions supporting credentials and tax regulations. States may form regional alliances to support these functions. Each state coordinates with other states, regional alliances, and CVISN Core Infrastructure systems to support nationwide access to credentials information for administrative and enforcement functions.

When building a credentialing system, it is useful to think about the process of ESE as part of the design criteria. The requirements for ESE have been moved to the section on electronic screening.

FMCSA's policy on electronic credentials administration between motor carriers and states is:

- FMCSA requires that states implement either a person-to-computer or a computer-to-computer interface.
- FMCSA recommends that states survey their stakeholders to determine whether both interfaces would be appropriate.

The concepts in Table 4.3–1 are based on an interpretation of the guiding principles and existing and emerging technologies. The guiding principles and operational concepts led to the system design requirements. The operational concepts are not testable.

Table 4.3–1
CV Administration Operational Concepts

Commit Level (F/P/N)	Item #	CV Administration Operational Concepts Compatibility Criteria	Req Level (Core/ Expanded)	Comments
	1.	Credential applications and fuel tax returns are filed electronically from CVO stakeholder facilities.	Core	
	2.	Internal state administrative processes are supported through electronic exchange of application data, safety records, carrier background data, and other government-held records.	Core	
	3.	IRP and IFTA base jurisdiction agreements are supported electronically.	Core	
	4.	Credential and fuel tax payment status information for interstate operators are made available electronically nationally to qualified stakeholders in accordance with privacy agreements.	Core	
	5.	User access to credential data is controlled (restricted and/or monitored) where necessary.	Core	
	6.	Mechanisms are made available for operators to dispute credentials records held by government systems.	Core	
	7.	Fees and taxes are paid electronically.	Expanded	
	8.	Electronic access to administrative processes and information is available from “one stop shops” in public sites.	Expanded	
	9.	Credential and fuel tax payment status information for intrastate operators are made available electronically to qualified stakeholders throughout the state.	Expanded	
	10.	Carrier audits are accomplished with electronic support.	Expanded	
	11.	The “paperless vehicle” concept is supported, i.e., electronic records become primary and paper records become secondary.	Expanded	

Note: F – Full Commitment; P – Partial Commitment; N – No Commitment
Core – Core CVISN; Expanded – Expanded CVISN capability
Complete code descriptions are given in Section 1.4.

Core CVISN state CV administration systems design requirements can be summarized as follows:

- Automated electronic processing via Web-based or computer-to-computer solutions from carrier to state (processing includes carrier application, state application processing, credential issuance, and tax filing) of at least IRP and IFTA credentials; ready to extend to other credentials [intrastate, titling, oversize/overweight (OS/OW), carrier registration, and HazMat]. Note: processing does not necessarily include e-payment.
- Update SAFER with credential information for interstate operators as actions are taken.
- Update CVIEW (or equivalent) with interstate and intrastate credential information as actions are taken.
- Connection to IRP and IFTA Clearinghouses.
- At least 10 percent of the transaction volume handled electronically; ready to bring on more carriers as carriers sign up; ready to extend to branch offices where applicable.

The state systems requirements in Table 4.3–2 apply to the design of state credentials-related systems. The table shows more detail about what "Core CVISN" means. The Core CVISN requirements are marked with "Core" in the fourth column [Req Level (Core/Expanded)]. For an overview of Core CVISN, see the *Introductory Guide to CVISN* [Reference 2].

Table 4.3–2
State CV Administration Systems Design Requirements Checklist

Commit Level (F/P/N)	Item #	State CV Administration Systems Design Requirements Checklist Compatibility Criteria	Req Level (Core/ Expanded)	Verification (T/I/D)	Comments
	4.3.1	Support electronic credentialing (electronic submission of applications, evaluation, processing, and application response) for IRP. (Either a Web-based or a computer-to-computer interface is required for Core CVISN.)	Core	T/D	
	~~1~~	~~Provide a Web site for a person-to-computer process. (Either a Web-based or a computer-to-computer interface is required for L1.)~~	~~L1~~ ~~CR 94~~	~~T~~	Requirement deleted.
	~~2~~	~~Provide a computer-to-computer automated process. (Either a Web-based or a computer-to-computer interface is required for L1.)~~	~~L1~~ ~~CR 94~~	~~T~~	Requirement deleted.
	~~2a~~	~~Use EDI standards to provide a computer-to-computer automated process.~~	~~L1~~ ~~CR 94~~	~~T~~	Requirement deleted.
	~~2b~~	~~Use XML standards to provide a computer-to-computer automated process.~~	~~E~~		Requirement deleted.
	4.3.2	Proactively provide updates to vehicle snapshots as needed when IRP credentials actions are taken.	Core	T	
	1	Interface to SAFER for interstate vehicle snapshots, using available SAFER interface from CVIEW or CVIEW-equivalent system.	Core	T	
	4.3.3	Proactively provide updates to carrier snapshots as needed when IRP credentials actions are taken.	Core	T	
	1	Interface to SAFER for interstate carrier snapshots, using available SAFER interface from CVIEW or CVIEW-equivalent system.	Core	T	
	4.3.4	Provide IRP Clearinghouse with IRP credential application information (recaps).	Core	D	

Commit Level (F/P/N)	Item #	State CV Administration Systems Design Requirements Checklist Compatibility Criteria	Req Level (Core/ Expanded)	Verification (T/I/D)	Comments
	4.3.5	Review fees billed and/or collected by a jurisdiction and the portion due other jurisdictions (transmittals) as provided by the IRP Clearinghouse.	Core	D	
	4.3.6	Support electronic jurisdiction-to-jurisdiction fee payments via IRP Clearinghouse.	Core	I	
	4.3.7	Support electronic credentialing (electronic submission of applications, evaluation, processing, and application response) for IFTA registration. (Either a Web-based or a computer-to-computer interface is required for Core CVISN.)	Core	T/D	
	~~1~~	~~Provide a Web site for a person-to-computer process. (Either a Web-based or a computer-to-computer interface is required for L1.)~~	~~L1~~ ~~CR 94~~	~~T~~	Requirement deleted.
	~~2~~	~~Provide a computer-to-computer automated process. (Either a Web-based or a computer-to-computer interface is required for L1.)~~	~~L1~~ ~~CR 94~~	~~T~~	Requirement deleted.
	~~2a~~	~~Use EDI standards to provide a computer-to-computer automated process.~~	~~L1~~ ~~CR 94~~	~~T~~	Requirement deleted.
	~~2b~~	~~Use XML standards to provide a computer-to-computer automated process.~~	~~E~~		Requirement deleted.
	4.3.8	Proactively provide updates to carrier snapshots as needed when IFTA credentials actions are taken or tax payments are made.	Core	T	
	1	Interface to SAFER for interstate carrier snapshots, using available SAFER interface.	Core	T	
	4.3.9	Provide IFTA Clearinghouse with IFTA credential application information using available interface.	Core	D	

Commit Level (F/P/N)	Item #	State CV Administration Systems Design Requirements Checklist Compatibility Criteria	Req Level (Core/ Expanded)	Verification (T/I/D)	Comments
	4.3.10	Support electronic tax filing for IFTA quarterly fuel tax returns. (Either a Web-based or a computer-to-computer interface is required for Core CVISN.)	Core	T/D	
	~~1~~	~~Provide a Web site for a person-to-computer process. (Either a Web-based or a computer-to-computer interface is required for L1.)~~	~~L1~~ ~~CR 94~~	~~T~~	Requirement deleted.
	~~2~~	~~Provide a computer-to-computer automated process. (Either a Web-based or a computer-to-computer interface is required for L1.)~~	~~L1~~ ~~CR 94~~	~~T~~	Requirement deleted.
	~~2a~~	~~Use EDI standards to provide a computer-to-computer automated process.~~	~~L1~~ ~~CR 94~~	~~T~~	Requirement deleted.
	~~2b~~	~~Use XML standards to provide a computer-to-computer automated process.~~	~~E~~		Requirement deleted.
	4.3.11	Provide information on taxes collected by own jurisdiction and the portion due other jurisdictions (transmittals) to the IFTA Clearinghouse using available interface.	Core	I	
	4.3.12	Download for automated review the demographic information from the IFTA Clearinghouse.	Core	D	
	4.3.13	Download for automated review the transmittal information from the IFTA Clearinghouse.	Core	D	
	4.3.14	Retrieve IFTA tax rate information electronically from IFTA, Inc.	Core	D	
	4.3.15	Support electronic credentialing (electronic submission of applications, evaluation, processing, and application response) for other credentials.	Expanded		
	1	Interstate carrier registration	Expanded		
	2	Intrastate carrier registration	Expanded		
	3	Vehicle title	Expanded		
	4	Intrastate vehicle registration	Expanded		

Commit Level (F/P/N)	Item #	State CV Administration Systems Design Requirements Checklist Compatibility Criteria	Req Level (Core/ Expanded)	Verification (T/I/D)	Comments
	5	HazMat credentialing/permitting, if such credentials/permits are required by state law	Expanded		
	6	Oversize/overweight permitting	Expanded		
	4.3.16	Proactively provide updates to vehicle snapshots as needed when credentials actions are taken.	Expanded		
	1	Vehicle title	Expanded		
	2	Intrastate vehicle registration	Expanded		
	3	Oversize/overweight permitting	Expanded		
	4.3.17	Proactively provide updates to carrier snapshots as needed when credentials actions are taken.	Expanded		
	1	Interstate carrier registration	Expanded		
	2	Intrastate carrier registration	Expanded		
	3	HazMat credentialing/permitting, if such credentials/permits are required by state law	Expanded		
	4	Oversize/overweight permitting	Expanded		
	4.3.18	Allow CV operators, government-operated, or third party systems to submit one or more applications in a single transaction.	Expanded		
	4.3.19	Provide commercial driver information to other jurisdictions via Commercial Driver's License Information System (CDLIS).	Core	D	
	4.3.20	Evaluate carrier safety performance prior to issuing vehicle registration renewal [i.e., support Performance and Registration Information Systems Management (PRISM) processes or equivalent].	Expanded		
	4.3.21	Allow carriers to provide information for audits electronically.	Expanded		
	4.3.22	Provide titling information to other jurisdictions via National Motor Vehicle Title Information System (NMVTIS).	Expanded		

Commit Level (F/P/N)	Item #	State CV Administration Systems Design Requirements Checklist Compatibility Criteria	Req Level (Core/ Expanded)	Verification (T/I/D)	Comments
	~~4.3.23~~	~~Provide revoked IFTA motor carrier information to other jurisdictions via State On-line Enforcement System (STOLEN).~~	~~Core~~		Requirement deleted.
	4.3.24	Accept electronic credential and supporting electronic documentation in lieu of paper versions.	Expanded		
	4.3.25	Proactively provide updates to driver snapshots as needed when credentials actions are taken.	Expanded		
	1	Interface to SAFER for driver snapshots using available SAFER interface.	Expanded		

Note: F – Full Commitment; P – Partial Commitment; N – No Commitment
Core – Core CVISN; Expanded – Expanded CVISN capability
T – interoperability Testing; I – Inspection of documentation; D – Demonstration
Complete code descriptions are given in Section 1.4.

4.4 State Electronic Screening Operational Concepts and Systems Design Requirements

The state electronic screening systems are likely to consist of:

- Screening System
- Roadside Operations System
- Sensor/Driver Communications System
- Electronic Screening Enrollment (ESE)

These electronic screening (e-screening) systems will operate at each fixed or mobile CV check station within a state. The systems perform roadside functions supporting automated carrier, vehicle, and driver identification and associated look-ups in infrastructure-supplied data for credentials and safety checks.

When building an electronic screening system, it is useful to think about e-screening enrollment (ESE) as part of the process. The requirements for ESE appear in this section. The requirements for ESE should be considered during design of other administrative and credentialing systems.

The concepts in Table 4.4–1 are based on an interpretation of the guiding principles and existing and emerging technologies. The guiding principles and operational concepts led to the system design requirements. The operational concepts are not testable.

Table 4.4–1
Electronic Screening Operational Concepts

Commit Level (F/P/N)	Item #	Electronic Screening Operational Concepts Compatibility Criteria	Req Level (Core/ Expanded)	Comments
	1.	Widespread participation in electronic screening programs is encouraged.	Core	
	2.	Jurisdictions disclose practices related to electronic screening.	Core	
	3.	Electronic screening is provided for vehicles equipped with FHWA-specified DSRC transponders. See Reference 15	Core	
	4.	Jurisdictions and/or e-screening programs provide a single point of contact for motor carriers to request enrollment in all jurisdictions' electronic screening programs.	Core	
	5.	If one jurisdiction or e-screening program provides a transponder to a carrier, it allows the carrier to use that transponder in other jurisdictions' e-screening programs and in other applications such as electronic toll collection.	Core	
	6.	For an enrolled carrier that has vehicles equipped with compatible transponders, jurisdictions and/or e-screening programs provide a mechanism for participation in electronic screening using those transponders.	Core	
	7.	Credentials and safety checks are conducted as part of the screening process.	Core	
	8.	Fixed and/or mobile roadside check stations are employed for electronic screening functions, according to the jurisdiction's needs and resources.	Core	
	9.	Jurisdictions support a common set of screening criteria.	Expanded	
	10.	Screening systems are interoperable with those in different jurisdictions.	Expanded	
	11.	Electronic screening is provided using license plate readers or technology other than DSRC transponders.	Expanded	

Note: F – Full Commitment; P – Partial Commitment; N – No Commitment
Core – Core CVISN; Expanded – Expanded CVISN capability
Complete code descriptions are given in Section 1.4.

Core CVISN state electronic screening systems design requirements can be summarized as follows:

- Use CVO credential and safety data (snapshots) to support screening decisions.
- Implemented at a minimum of one fixed or mobile inspection site.
- Ready to replicate at other sites.

The state systems requirements in Table 4.4–2 apply to the design of state screening-related systems. The table shows more detail about what "Core CVISN" means. The Core CVISN requirements are marked with "Core" in the fourth column [Req Level (Core/Expanded)]. For an overview of Core CVISN, see the *Introductory Guide to CVISN* [Reference 2].

Table 4.4–2
State Electronic Screening Systems Design Requirements Checklist

Commit Level (F/P/N)	Item #	State Electronic Screening Systems Design Requirements Checklist Compatibility Criteria	Req Level (Core/ Expanded)	Verification (T/I/D)	Comments
	4.4.1	Follow FHWA guidelines for DSRC equipment.	Core		
	1	For the immediate future, all CVO and Border Crossing projects will continue to utilize the current DSRC configuration employed by the programs. This is the "American Society for Testing and Materials (ASTM) E17.51 version 6" active tag. (The DSRC provisional standard is defined in the FHWA specification [Reference 15].)	Core	D	
	2	~~Be prepared to transition to the sandwich specification after rulemaking is complete. [See the Notice of Proposed Rulemaking (NPRM) regarding DSRC in ITS CVO [Reference 14].]~~			
	2a	~~The new ASTM Physical Layer in the active mode [Reference 11];~~	~~Expanded~~		
	2b	~~the existing ASTM Version 6 Data Link layer in the synchronous mode [Reference 12];~~	~~Expanded~~		

Commit Level (F/P/N)	Item #	State Electronic Screening Systems Design Requirements Checklist Compatibility Criteria	Req Level (Core/ Expanded)	Verification (T/I/D)	Comments
	2c	~~and the Institute of Electrical and Electronics Engineers (IEEE) 1455 Application Layer [Reference 13].~~	~~Expanded~~		
	4.4.2	Use snapshots updated by a SAFER/CVIEW subscription in an automated process to support screening decisions.			
	1	Carrier snapshots	Core	T/D	
	2	Vehicle snapshots	Core	T/D	
	3	Driver snapshots	Expanded		
	4.4.3	*Requirement deleted in previous version of this document.*			
	1	*Requirement deleted in previous version of this document.*			
	4.4.4	At one or more sites, provide electronic mainline or ramp screening for transponder-equipped vehicles, and clear for bypass if carrier and vehicle were properly identified and screening criteria were passed.	Core	T/D	
	1	For transponder-equipped vehicles, identify carrier at mainline or ramp speeds.	Core	T/D	
	2	For transponder-equipped vehicles, identify vehicle at mainline or ramp speeds.	Core	T/D	
	3	Use Weigh-In-Motion (WIM) or weight history at mainline speed or on the ramp in making screening decisions.	Core	I/D	
	4	Use safety data from snapshots and other sources.	Core	T/D	
	5	Use credentials data from snapshots and other sources.	Core	T/D	
	6	Record screening event data.	Expanded		

Commit Level (F/P/N)	Item #	State Electronic Screening Systems Design Requirements Checklist Compatibility Criteria	Req Level (Core/ Expanded)	Verification (T/I/D)	Comments
	7	For transponder-equipped vehicles, identify driver at mainline or ramp speeds.	Expanded		
	4.4.5	Carrier enrollment: Collect from the carrier a list of jurisdictions and/or e-screening programs in which it wishes to participate. Inform those jurisdictions and/or e-screening programs.	Core	D/I	
	4.4.6	Vehicle enrollment: Collect from the carrier a list of the vehicles for each jurisdiction and/or e-screening program. Inform those jurisdictions and/or e-screening programs.	Core	D/I	
	4.4.7	Record transponder number and default carrier ID for each vehicle that intends to participate in e-screening.	Core	D/I	
	4.4.8	Share carrier ID for each carrier that intends to participate in e-screening with other jurisdictions and/or e-screening programs as requested by the carrier.	Core	D/I	
	1	Share the information via SAFER snapshots.	Expanded		
	4.4.9	Share transponder number and default carrier ID for each vehicle that intends to participate in e-screening with other jurisdictions, e-screening programs, or other agencies as requested by the carrier.	Core	D/I	
	1	Share the information via SAFER snapshots.	Expanded		
	4.4.10	Accept each qualified vehicle already equipped with a compatible transponder into your e-screening program without requiring an additional transponder.	Core	D/I	

Commit Level (F/P/N)	Item #	State Electronic Screening Systems Design Requirements Checklist Compatibility Criteria	Req Level (Core/ Expanded)	Verification (T/I/D)	Comments
	4.4.11	Enable the carrier to share information about the transponder that you issue with other jurisdictions, e-screening programs, or agencies.	Core	D/I	
	4.4.12	Verify credentials/safety information with authoritative source prior to issuing citation.	Core	D/I	
	4.4.13	If a vehicle illegally bypasses or leaves the CV check station, alert law enforcement for possible apprehension.	Expanded		
	4.4.14	Report periodically to state safety information system on the activities conducted at each station (e.g., statistics).	Expanded		

Note: F – Full Commitment; P – Partial Commitment; N – No Commitment;
Core – Core CVISN; Expanded – Expanded CVISN capability
T – interoperability Testing; I – Inspection of documentation; D – Demonstration
Complete code descriptions are given in Section 1.4.

5. DATA MAINTENANCE REQUIREMENTS

The checklist in this chapter (formerly documented in *COACH Part 3* [Reference 19]) summarizes the requirements for maintaining data and sharing updates with other CVO stakeholders. Systems should be designed to meet these criteria. If a user group has more stringent requirements, those requirements override these and should be noted in the "Comments" column.

Table 5–1 Data Maintenance & Update

Commit Level (F/P/N)	Data Need Category	Requirement for data to be maintained or updated	Reqts Level	Comments
	Routine snapshot changes are those for which users can wait until the next routine snapshot update is scheduled. Routine snapshot data changes include updates related to passed inspections, compliance reviews, or credential renewals or supplements.	The authoritative source system should update the snapshot record within 24 hours of the change.	Core; Expanded	Core for carrier and vehicle snapshots; Expanded for driver snapshots
	High-priority snapshot changes are those that users need to know about immediately. High priority snapshot data changes include out-of-service (OOS) resulting from an inspection.	The source system should update the snapshot record within 30 minutes of the change.	Core; Expanded	Core for carrier and vehicle snapshots; Expanded for driver snapshots
	Snapshot subscription fulfillment is the SAFER or CVIEW process for sending specified snapshot output views to users based on standing requests to do so when specified data changes.	Whenever the criteria for sending a snapshot are triggered, the snapshot system (CVIEW or SAFER) should distribute the revised snapshot within 24 hours for routine snapshot changes and within 30 minutes for high-priority snapshot changes.	Core; Expanded	Core for carrier and vehicle snapshots; Expanded for driver snapshots

Commit Level (F/P/N)	Data Need Category	Requirement for data to be maintained or updated	Reqts Level	Comments
	An inspection report indicates the results of an inspection conducted at the roadside by a qualified inspector.	Normally, the results of an inspection using ASPEN should be reported electronically within 24 hours of being conducted. If the vehicle or driver was placed OOS, the results should be reported within 30 minutes.	Core	
	Credential application response is the response from the state to the applicant. In this context, the "response" reflects the results of evaluating the credential application.	The state system should respond to the applicant's system within 2 hours for a correct transaction that requires no manual intervention. If manual intervention is required, the state system should respond to the applicant's system within 24 hours of receipt of an electronic input.	Core	
	IRP base jurisdiction agreement data are the data required by foreign jurisdictions to understand the fees collected and calculated on their behalf. In IRP lingo, the data are exchanged via recaps.	The jurisdiction IRP system should send recaps to the IRP Clearinghouse by the 10th calendar day of each month.	Core	
	IFTA base jurisdiction agreement data are those data required by other jurisdictions to understand the quarterly fuel taxes collected on their behalf. In IFTA lingo, these data are called "demographic" for basic census information and "transmittal" for tax return information.	The jurisdiction IFTA system should send updated demographic daily or as changes occur, and should send transmittal and summary total data to the IFTA Clearinghouse monthly.	Core	

Commit Level (F/P/N)	Data Need Category	Requirement for data to be maintained or updated	Reqts Level	Comments
	The *Privacy Act of 1974* [Reference 18] attempts to regulate the collection, maintenance, use, and dissemination of personal information by federal government agencies. Federal systems must adhere to the law. Some sections of the law apply to state and local governments as well. Additionally, some states have related laws regarding privacy and data access.	The systems affected by the Act or related statutes should incorporate procedures, protocols, and designs that support the law. The Privacy Act includes sections concerning data disclosure, accounting of disclosure, access, amendment, reporting, archiving, and other activities.	Core	

6. REFERENCES

1. JHU/APL, *ITS/CVO Commercial Vehicle Information Systems and Networks (CVISN) Glossary*, POR-96-6997 V2.0, December 2000. (Delivered via SSD-PL-00-0751, 16 February 2001.) [Note: This document is scheduled to be revised in 2008.] The latest version will be available on the Federal Motor Carrier Safety Administration (FMCSA) CVISN Web site.
2. JHU/APL, *Introductory Guide to CVISN*, POR-99-7186 P.2, February 2000. (Delivered via SSD/PL-00-0010, 21 January 2000.) [Note: This document is scheduled to be revised in 2008.] The latest version will be available on the Federal Motor Carrier Safety Administration (FMCSA) CVISN Web site.
3. JHU/APL, *Commercial Vehicle Information Systems and Networks (CVISN) System Design Description*, POR-97-6998 V3.0, April 2003. (Delivered via SSD-PL-03-0123.) [Note: This document is scheduled to be revised in 2008.] The latest version will be available on the Federal Motor Carrier Safety Administration (FMCSA) CVISN Web site.
4. John A. Volpe National Transportation Systems Center (Volpe Center), *Safety and Fitness Electronic Records (SAFER) Interface Certification Procedure (ICP)* Version 1.0, July 2003. The latest version will be available on the Federal Motor Carrier Safety Administration (FMCSA) CVISN Web site.
5. Volpe Center, *SAFER Commercial Vehicle Information Exchange Window (CVIEW) Interface Re-Certification*, v7, January 2008. The latest version will be available on the Federal Motor Carrier Safety Administration (FMCSA) CVISN Web site.
6. Volpe Center, *SAFER CVISN State Data Baseline Procedure*, Version 1.0, March 2008. The latest version will be available on the Federal Motor Carrier Safety Administration (FMCSA) CVISN Web site.
7. Intelligent Transportation Society of America, *ITS CVO Guiding Principles*, last updated 27 March 1998.
8. Intelligent Transportation Society of America, *Fair Information Principles for ITS/CVO*, last updated 12 January 1999.
9. Intelligent Transportation Society of America, *Interim ITS/CVO Interoperability Guiding Principles*, last updated 12 January 1999.
10. JHU/APL, *Commercial Vehicle Information Systems and Networks (CVISN) Architecture [Revised]*, POR-02-7364 V3.0, December 2006. The latest version will be available on the Federal Motor Carrier Safety Administration (FMCSA) CVISN Web site.
11. Reference deleted.
12. Reference deleted.
13. Reference deleted.

14. Reference deleted.

15. JHU/APL, *Draft Specification for Dedicated Short Range Communications (DSRC) for Commercial Vehicles*, V0.0.1, November 1999. (Delivered via SSD-PL-99-0784, 30 December 1999.) The latest version will be available on the Federal Motor Carrier Safety Administration (FMCSA) CVISN Web site.

16. Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (SAFETEA-LU). Available from the FHWA Web site http://www.fhwa.dot.gov/safetealu/index.htm.

17. Volpe Center, *SAFER Interface Control Document*, Version 8.1, March 2008. The latest version will be available on the Federal Motor Carrier Safety Administration (FMCSA) CVISN Web site.

18. *The Privacy Act of 1974*, 5 U.S.C. § 552a (1994 & Supp. II 1996) (amended 1997, 5 U.S.C.A. § 552a (West Supp. 1998)), which became effective on September 27, 1975, can generally be characterized as an omnibus "code of fair information practices" which attempts to regulate the collection, maintenance, use, and dissemination of personal information by federal government agencies. An overview of the *Privacy Act of 1974*, prepared in September 1998 by the Office of Information and Privacy in coordination with the Office of Management and Budget is available on the Web at http://www.usdoj.gov/oip/04_7_1.html.

19. JHU/APL, *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 3 – Detailed System Checklists*, POR-97-7067 V2.0, August 2003. (Delivered via SSD-PL-03-0472, 22 October 2003.) [Note: This document is no longer being maintained. The archive contains this obsolete version.].

APPENDIX A. CORE CVISN CHECKLIST

Checklist to Document States' Deployment of Core CVISN Capabilities

The Federal Motor Carrier Safety Administration (FMCSA) has defined a set of CVISN capabilities that can be deployed incrementally by a state and its motor carriers. These "Core" capabilities focus on electronically exchanging safety and credentialing information, electronically processing interstate registration and fuel tax credentials, and implementing roadside electronic screening at one fixed or mobile site.

Detailed requirements for Core CVISN are provided in the *CVISN Operational and Architectural Compatibility Handbook (COACH), Part 1*.

To implement the provisions of the Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (SAFETEA-LU) (Section 4126) [Reference 16], FMCSA has developed interoperability tests to verify that state systems conform with the CVISN aspects of the National ITS Architecture, applicable standards, and protocols. Interoperability tests have been developed that verify that the intended interfaces were implemented correctly and that the systems operate together to accomplish shared functions. There are two types of interoperability tests:

- Pair-wise tests verify interfaces between selected pairs of deployed systems. FMCSA expects that the state will conduct pair-wise tests through the various stages of its CVISN deployment. FMCSA requires certification of the state's CVIEW or CVIEW-equivalent system interface to SAFER.
- End-to-end tests verify dataflow and data usage among several selected systems. Recommended end-to-end tests are described in Appendix B.

The guidelines, roles, and responsibilities in accomplishing the CVISN interoperability tests and completing the Core CVISN checklist are identified below:

- A representative of the state's FMCSA Division Office (Division Administrator, State Director, or designee) will work with the state to introduce the concepts of CVISN interoperability testing, make sure the tests are planned and conducted, and report the success of the tests to FMCSA's Office of Analysis, Research and Technology.
- The ITS/CVO Specialist from the FMCSA Service Center will be available to support the Division Office staff in answering questions.

- States will document the tests' results to the FMCSA Division Office and summarize testing activities. States are encouraged to share lessons learned during the monthly CVISN program managers' teleconferences and in other appropriate meetings [Commercial Vehicle Safety Alliance (CVSA), ITS America, CVISN Deployment Forums, etc.].
- States will work with the John A. Volpe National Transportation Systems Center (Volpe Center) to execute the SAFER Interface Certification tests [References 4 and 17], tailored as needed to match their own system implementations. Upon successful completion of the SAFER Interface Certification testing, the Volpe Center will submit a request to the FMCSA for approval of the CVIEW or CVIEW-equivalent system in question. If the request is approved, the FMCSA will notify the state and the Volpe Center that the referenced system has been certified to exchange information with the SAFER production system. The Volpe Center will then coordinate the commencement of that state's CVIEW transactions with SAFER.
- Upon reviewing the Core CVISN checklist documentation provided from the state's FMCSA Division Office, FMCSA's Office of Analysis, Research and Technology will provide a letter to the state acknowledging that it has successfully implemented CVISN Core capabilities and has completed the required interoperability tests.

How Does a State Verify Conformance with Core CVISN?

The four tables in this checklist present the Core CVISN capabilities paired with required and recommended tests or demonstrations that the states can carry out in order to show achievement of Core CVISN deployment. The requirements listed in the tables are extracted from the State Systems Design Requirements Checklist (Tables 4.1–2, 4.2–2, 4.3–2, and 4.4–2) of CVISN *COACH Part 1*. This checklist is for states to use to easily correlate the Core CVISN requirements to interoperability tests and to check off tests and demonstrations as they are completed.

The four tables are:

- Table A–1. General State Systems Design Requirements Checklist
- Table A–2. State Safety Information Exchange and Safety Assurance Systems Design Requirements Checklist
- Table A–3. State Commercial Vehicle (CV) Administration Systems Design Requirements Checklist
- Table A–4. State Electronic Screening Systems Design Requirements Checklist

The format of the tables is as follows:

- Column 1 “Check When Done” provides a place for the state to check off that a capability fulfilling a Core CVISN requirement has been tested.
- Column 2 “Item #” specifies the Item Number in the corresponding tables in *COACH Part 1*; the numbers are not always sequential, because *COACH Part 1* also includes capabilities beyond Core CVISN, which are not included in these checklists.
- Column 3 “Compatibility Criteria” lists the requirements from *COACH Part 1*.
- Column 4 “Required Core CVISN Interoperability Tests” provides a list of required tests or demonstrations/inspections to verify achievement of the Core CVISN capabilities. A place is provided for states to note the date of completion of the tests. If the cell is gray, then no required test is defined at that level.
- Column 5 “Comments” provides a place for the state to explain their entry in column 4.

The following abbreviations are used in the Interoperability Test columns of the tables:

- ETE = End-to-End interoperability tests
- WETE = Web-based End-to-End interoperability tests

Please refer to the *ITS/CVO CVISN Glossary* [Reference 1] for other acronyms that may be used in this document.

Table A–1. General State Systems Design Requirements Checklist

Tests associated with the requirements in this table are addressed in the subsequent tables. It is still recommended that you check off the items in this table as the related tests are completed.

The Core CVISN capabilities addressed in this table apply to the design of all state systems; they are summarized as follows:

- An organizational framework for cooperative system development has been established among state agencies and motor carriers.
- A state CVISN System Design has been established that conforms to the CVISN Architecture and can evolve to include new technology and capabilities.
- All the elements of three Core CVISN capability areas (Safety Information Exchange, Credentials Administration, and Electronic Screening) have been implemented using applicable architectural guidelines, operational concepts, and standards.

Table A–1.
General State Systems Design Requirements Checklist

Check When Done	Item #	Compatibility Criteria	Required Core CVISN Interoperability Tests (or other method of verifying capability)	Comments
	4.1.1	Adopt standard identifiers for carriers, vehicles, drivers, and transponders to support information exchange.		
	1	Adopt standard identifiers for interstate carrier, vehicle, driver, and transponder.		
	4.1.2	Use the World Wide Web for person-to-computer interactions between private citizens and state information systems.		
	4.1.3	Use open standards for computer-to-computer exchange of information with other jurisdictions and with the public.		
	1	Use open standards[1] for transactions between state information systems and private systems (CV operators, insurance companies, etc.).		
	2	Use open standards for transactions between state information systems and CVISN Core Infrastructure systems, where available.		
	4.1.4	Ensure that all information transfers, fee payments, and money transfers are authorized and secure, e.g., through access control and encryption.		

Check When Done	Item #	Compatibility Criteria	Required Core CVISN Interoperability Tests (or other method of verifying capability)	Comments
	4.1.5	Exchange safety and credentials data electronically within the state to support credentialing, safety, and other roadside functions. Where useful, exchange snapshots.		
	1	Data for interstate carriers		
	2	Data for interstate vehicles		
	3	Data for intrastate carriers		
	4	Data for intrastate vehicles		
	4.1.6	Demonstrate technical interoperability by performing Interoperability Tests.		

[1] Open standards are publicly available specifications or standards that promote interoperability.

Table A–2. State Safety Information Exchange and Safety Assurance Systems Design Requirements Checklist

The Core CVISN capabilities addressed in this table apply to the design of state safety-related systems; they are summarized as follows:

- Inspection reporting using ASPEN (or equivalent) at all major inspection sites. ASPEN data sent to SAFER directly or indirectly.
- Connection to SAFER system to provide exchange of interstate carrier and vehicle data snapshots among states.
- Implementation of the CVIEW (or equivalent) system for exchange of intrastate and interstate data within state and connection to SAFER for exchange of interstate data through snapshots.

Table A–2.
State Safety Information Exchange and Safety Assurance Systems Design Requirements Checklist

Check When Done	Item #	Compatibility Criteria	Required Core CVISN Interoperability Tests (or other method of verifying capability)	Comments
	4.2.1	Use ASPEN (or equivalent) at all major inspection sites	**Date ASPEN/equivalent implemented:** _____	
	1	Select vehicles and drivers for inspection based on availability of inspector, standard inspection selection system, vehicle measures, and random process, as statutes permit.		
	2	Report interstate inspections to Motor Carrier Management Information System (MCMIS) via SAFETYNET.		
	3	Report intrastate inspections to SAFETYNET.		
	4	Submit interstate and intrastate inspections for temporary storage to SAFER.		

Check When Done	Item #	Compatibility Criteria	Required Core CVISN Interoperability Tests (or other method of verifying capability)	Comments
	4.2.2	SAFETYNET submits inspection reports to SAFER.		
	1	SAFETYNET submits interstate inspection reports to SAFER.	▪ Demonstration or inspection of state system design documents **Date Completed:** _____	
	2	SAFETYNET submits intrastate inspection reports to SAFER.	▪ Demonstration or inspection of state system design documents **Date Completed:** _____	
	4.2.4	Use Compliance Analysis Performance Review Information (CAPRI) (or equivalent) for compliance reviews.	**Date CAPRI Implemented:** _____	
	1	Report interstate compliance reviews to MCMIS via SAFETYNET.		
	4.2.9	Implement the CVIEW (or equivalent) system for exchange of intrastate and interstate data within state and connection to SAFER for exchange of interstate data through snapshots	**Complete SAFER interface certification with the Volpe Center (Reference 4)** **Date Completed:** _____ **Note:** ▪ Tests associated with credential snapshot updates to CVIEW and SAFER are addressed in the Credentials Administration capability area.	
	1	Implement a state CVIEW.		
	2	Implement a CVIEW equivalent system.		
	3	Utilize the SAFER option.		

Table A–3. State CV Administration Systems Design Requirements Checklist

The Core CVISN capabilities addressed in this table apply to the design of state credentials-related systems; they are summarized as follows:

- Automated electronic processing via Web-based or computer-to-computer solutions from carrier to state (processing includes carrier application, state application processing, credential issuance, and tax filing) of at least International Registration Plan (IRP) and International Fuel Tax Agreement (IFTA) credentials; ready to extend to other credentials [intrastate, titling, oversize/overweight (OS/OW), carrier registration, and HazMat]. Note: processing does not necessarily include electronic payment.
- Update SAFER with credential information for interstate operators as actions are taken.
- Update CVIEW (or equivalent) with interstate and intrastate credential information as actions are taken.
- Connection to IRP and IFTA Clearinghouses.
- At least 10 percent of the transaction volume handled electronically; ready to bring on more carriers as carriers sign up; ready to extend to branch offices where applicable.

Also note that the requirements for electronic screening enrollment (ESE) are included in Table A–4 with requirements for state screening-related systems.

Table A–3.
State CV Administration Systems Design Requirements Checklist

Check When Done	Item #	Compatibility Criteria	Required Core CVISN Interoperability Tests (or other method of verifying capability)	Comments
	4.3.1	Support electronic credentialing (electronic submission of applications, evaluation, processing, and application response) for IRP. Either a Web-based or a computer-to-computer interface is required for Core CVISN deployment.	**For Web-based credential applications:** ▪ Scenario WETE-01, 04, 05, 11 **For designs that implement computer-computer interfaces between carrier and state:** ▪ Scenario ETE-01, 04, 05, 11 **Date Completed:** _____	
	4.3.2	Proactively provide updates to vehicle snapshots as needed when IRP credentials actions are taken.	**For Web-based credential applications:** ▪ Scenario WETE-01, 04, 05, 11 **For designs that implement computer-computer interfaces between carrier and state:** ▪ Scenario ETE-01, 04, 05, 11 **Date Completed:** _____	
	1	Interface to SAFER for interstate vehicle snapshots, using available SAFER interface from CVIEW or CVIEW-equivalent system.		
	4.3.3	Proactively provide updates to carrier snapshots as needed when IRP credentials actions are taken.	**For Web-based credential applications:** ▪ Scenario WETE-01, 04, 05, 11 **For designs that implement computer-computer interfaces between carrier and state:** ▪ Scenario ETE-01, 04, 05, 11 **Date Completed:** _____	
	1	Interface to SAFER for interstate carrier snapshots, using available SAFER interface from CVIEW or CVIEW-equivalent system.		
	4.3.4	Provide IRP Clearinghouse with IRP credential application information (recaps).	▪ Demonstration of IRP Clearinghouse connection **Date Completed:** _____	
	4.3.5	Review fees billed and/or collected by a jurisdiction and the portion due other jurisdictions (transmittals) as provided by the IRP Clearinghouse.	▪ Demonstration of IRP Clearinghouse connection **Date Completed:** _____	

Check When Done	Item #	Compatibility Criteria	Required Core CVISN Interoperability Tests (or other method of verifying capability)	Comments
	4.3.6	Support electronic state-to-state fee payments via IRP Clearinghouse.	▪ Inspection of IRP Clearinghouse agreement **Date Completed:** _____	
	4.3.7	Support electronic credentialing (electronic submission of applications, evaluation, processing, and application response) for IFTA registration. Either a Web-based or a computer-to-computer interface is required for Core CVISN deployment.	**For Web-based credential applications:** ▪ Scenario WETE-06 (IFTA registration) **For designs that implement computer-computer interfaces between carrier and state:** ▪ Scenario ETE-06 **Date Completed:** _____	
	4.3.8	Proactively provide updates to carrier snapshots as needed when IFTA credentials actions are taken or tax payments are made.	**For Web-based credential applications:** ▪ Scenario WETE-06 (IFTA registration and quarterly tax filing) **For designs that implement computer-computer interfaces between carrier and state:** ▪ Scenario ETE-06 **Date Completed:** _____	
	1	Interface to SAFER for interstate carrier snapshots, using available SAFER interface.		
	4.3.9	Provide IFTA Clearinghouse with IFTA credential application information, using available interface.	▪ Demonstration of IFTA Clearinghouse connection **Date Completed:** _____	
	4.3.10	Support electronic tax filing for IFTA quarterly fuel tax returns. Either a Web-based or a computer-to-computer interface is required for Core CVISN deployment.	▪ Demonstration of electronic IFTA quarterly tax filing process **Date Completed:** _____	
	4.3.11	Provide information on taxes collected by own jurisdiction and the portion due other jurisdictions (transmittals) to the IFTA Clearinghouse, using available interface.	▪ Inspection of IFTA Clearinghouse agreement **Date Completed:** _____	

Check When Done	Item #	Compatibility Criteria	Required Core CVISN Interoperability Tests (or other method of verifying capability)	Comments
	4.3.12	Download for automated review the demographic information from the IFTA Clearinghouse.	▪ Demonstration of IFTA Clearinghouse connection **Date Completed:** _____	
	4.3.13	Download for automated review the transmittal information from the IFTA Clearinghouse.	▪ Demonstration of IFTA Clearinghouse connection **Date Completed:** _____	
	4.3.14	Retrieve IFTA tax rate information electronically from IFTA, Inc.	▪ Demonstration of IFTA Clearinghouse connection **Date Completed**: _____	
	4.3.19	Provide commercial driver information to other jurisdictions via Commercial Driver's License Information System (CDLIS).	▪ Does the state operate CDLIS? _____ **Yes** _____ **No** **Date Completed:** _____	

Table A–4. State Electronic Screening Systems Design Requirements Checklist

The Core CVISN capabilities addressed in this table apply to the design of state screening-related systems; they are summarized as follows:

- Use CVO credential and safety data (snapshots) to support screening decisions.
- Implemented at a minimum of one fixed or mobile inspection site.
- Ready to replicate at other sites.

The CVISN Architecture and standards provide the technical framework for any given roadside reader or interrogation device to meaningfully query, send or receive, and process data from any given transponder mounted in a vehicle, regardless of which manufacturer produced either the reader or transponder. The capabilities to electronically screen transponder-equipped commercial vehicles at one or more fixed or mobile sites and to replicate this at other sites are key premises of CVISN deployment. The FMCSA strongly supports electronic screening programs using various business models, including public-private partnerships such as the PrePass™ program, administered by Heavy Vehicle Electronic License Plate (HELP), Inc., and the North American Pre-clearance and Safety System (NORPASS), as well as other state-administered programs, such as Oregon's Green Light electronic screening system.

Table A–4.
State Electronic Screening Systems Design Requirements Checklist

Check When Done	Item #	Compatibility Criteria	Required Core CVISN Interoperability Tests (or other method of verifying capability)	Comments
	4.4.1	Follow FHWA guidelines for Dedicated Short Range Communications (DSRC) equipment.	▪ Inspection of tags **Date Completed:** _____	
	1	For the immediate future, all CVO and Border Crossing projects will continue to utilize the current DSRC configuration employed by the programs. This is the "American Society for Testing and Materials (ASTM) version 6" active tag. (The DSRC provisional standard is defined in the FHWA specification [Reference 15].)		
	4.4.2	Use snapshots updated by a SAFER/CVIEW subscription in an automated process to support screening decisions.	▪ Scenario ETE-03, Screening an Interstate Vehicle **Date Completed:** _____	
	1	Carrier snapshots.		
	2	Vehicle snapshots.		
	4.4.4	At one or more sites, provide electronic mainline or ramp screening for transponder-equipped vehicles, and clear for bypass if carrier and vehicle were properly identified and screening criteria were passed.		
	1	For transponder-equipped vehicles, identify carrier at mainline or ramp speeds.	▪ Scenario ETE-03, Screening an Interstate Vehicle **Date Completed:** _____	
	2	For transponder-equipped vehicles, identify vehicle at mainline or ramp speeds.		

Check When Done	Item #	Compatibility Criteria	Required Core CVISN Interoperability Tests (or other method of verifying capability)	Comments
	3	Use Weigh-In-Motion (WIM) at mainline speed or on the ramp, or weight history in making screening decisions.	▪ If weight is checked using WIM (mainline or ramp), inspection of screening displays; or ▪ Demonstration of process to check weight compliance **Date Completed:** _____	
	4	Use safety data from snapshots and other sources.	▪ Scenario ETE-03, Screening an Interstate Vehicle **Date Completed:** _____	
	5	Use credentials data from snapshots and other sources.		
	4.4.5	Carrier enrollment: Collect from the carrier a list of jurisdictions and/or e-screening programs in which it wishes to participate. Inform those jurisdictions and/or e-screening programs.	▪ Check if a member of: ♦ NORPASS: _____ ♦ PrePass™: _____ ; or ▪ If not a member of NORPASS or PrePass™, then demonstration or inspection of state system design documents **Date Completed:** _____	
	4.4.6	Vehicle enrollment: Collect from the carrier a list of the vehicles for each jurisdiction and/or e-screening program. Inform those jurisdictions and/or e-screening programs.	▪ Check if a member of: ♦ NORPASS: _____ ♦ PrePass™: _____ ; or ▪ If not a member of NORPASS or PrePass™, then demonstration or inspection of state system design documents **Date Completed:** _____	

Check When Done	Item #	Compatibility Criteria	Required Core CVISN Interoperability Tests (or other method of verifying capability)	Comments
	4.4.7	Record transponder number and default carrier ID for each vehicle that intends to participate in e-screening.	▪ Check if a member of: ♦ NORPASS: _____ ♦ PrePass™: _____ ; or ▪ If not a member of NORPASS or PrePass™, then demonstration or inspection of state system design documents **Date Completed:** _____	
	4.4.8	Share carrier ID for each carrier that intends to participate in e-screening with other jurisdictions and/or e-screening programs as requested by the carrier.	▪ Check if a member of: ♦ NORPASS: _____ ♦ PrePass™: _____ ; or ▪ If not a member of NORPASS or PrePass™, then demonstration or inspection of state system design documents **Date Completed:** _____	
	4.4.9	Share transponder number and default carrier ID for each vehicle that intends to participate in e-screening with other jurisdictions, e-screening programs, or other agencies as requested by the carrier.	▪ Check if a member of: ♦ NORPASS: _____ ♦ PrePass™: _____ ; or ▪ If not a member of NORPASS or PrePass™, then demonstration or inspection of state system design documents **Date Completed:** _____	
	4.4.10	Accept each qualified vehicle already equipped with a compatible transponder into your e-screening program without requiring an additional transponder.	▪ Check if a member of: ♦ NORPASS: _____ ♦ PrePass™: _____ ; or ▪ If not a member of NORPASS or PrePass™, then demonstration or inspection of state system design documents **Date Completed:** _____	

Check When Done	Item #	Compatibility Criteria	Required Core CVISN Interoperability Tests (or other method of verifying capability)	Comments
	4.4.11	Enable the carrier to share information about the transponder that you issue with other jurisdictions, e-screening programs, or agencies.	▪ Check if a member of: ♦ NORPASS: _____ ♦ PrePass™: _____ ; or ▪ If not a member of NORPASS or PrePass™, then demonstration or inspection of state system design documents **Date Completed:** _____	
	4.4.11	Verify credentials/safety information with authoritative source prior to issuing citation.	▪ Demonstration or inspection of procedures **Date Completed:** _____	

This Page Intentionally Blank

APPENDIX B. RECOMMENDED END-TO-END TESTS

End-to-End Tests

A key operational concept of CVISN is to share data among safety, credentialing and screening systems. Thus the tests of conformance for Core CVISN capabilities are the End-to-End (ETE) tests that demonstrate the sharing of data among systems. The end-to-end tests (denoted by scenarios labeled ETE and WETE here and in the tables of Appendix A) will demonstrate that data is shared and transferred through the applicable systems in order to carry out the desired function.

The recommended end-to-end tests are listed here and described below. While most states are implementing Web-based credentialing, both Web-based versions and computer-computer interface versions of the credential end-to-end interface tests are included here.

- ETE–01: Carrier Adds Vehicle (IRP Supplemental)
- ETE–03: Screening an Interstate Vehicle (note: Web-based test not applicable)
- ETE–04: Carrier Adds Jurisdiction (IRP Supplemental)
- ETE–05: Carrier Renews IRP Credential
- ETE–06: Carrier Renews IFTA Credential
- ETE–11: Carrier Adds More Than One Vehicle (IRP Supplemental)

- WETE–01: Carrier Adds Vehicle (IRP Supplemental)
- WETE–04: Carrier Adds Jurisdiction (IRP Supplemental)
- WETE–05: Carrier Renews IRP Credential
- WETE–06: Carrier Renews IFTA Credential
- WETE–11: Carrier Adds More Than One Vehicle (IRP Supplemental)

In the descriptions below, “State CVIEW System” refers to either the state’s CVIEW or CVIEW-equivalent system. These tests describe nominal configurations that a state may adjust for their own business purposes. Web services may be used rather than XML transactions.

ETE–01: Carrier Adds Vehicle (IRP Supplemental)

General Data Flow:
1. The carrier submits an IRP Supplemental Application for adding a vehicle.
2. The CV Administration performs status checks as required for the state IRP business processes.
3. If the application is approved, the CV Administration sends an invoice notice back to the carrier.
4. The carrier receives the invoice notice and sends payment information.
5. The CV Administration receives payment information and sends the credential to the carrier.
6. The CV Administration sends a vehicle snapshot update to the state CVIEW system.
7. The state CVIEW system sends a T0022 IRP Registration (Cab Card) Input Transaction to the SAFER system.
8. The state CVIEW system sends a vehicle snapshot to the Roadside Operations system.

ETE–03: Screening an Interstate Vehicle

General Data Flow:
1. Vehicles obtain a transponder and enroll in the screening program. Enrollment administration may be handled by the state, a third party administrator, or by a national program (e.g. PrePass or NORPASS).
2. On the highway, the vehicle's transponder ID is read by the screening system.
3. Screening software uses snapshot data from CVIEW or SAFER to make a screening decision.
4. A screening decision, i.e., "Bypass" or "Pull-In", is made and displayed to the vehicle operator.
5. The screening results are displayed at the Roadside Operations system.

ETE–04: Carrier Adds Jurisdiction (IRP Supplemental)

General Data Flow:
1. The carrier submits an IRP Supplemental Application for adding a jurisdiction.
2. The CV Administration performs status checks as required for the state IRP business processes.
3. If the application is approved, the CV Administration sends an invoice notice back to the carrier.
4. The carrier receives the invoice notice and sends payment information.
5. The CV Administration receives payment information and sends a credential to the carrier.
6. The CV Administration sends a snapshot update to the state CVIEW system.
7. The state CVIEW system sends a T0022 IRP Registration (Cab Card) Input Transaction to the SAFER system.
8. The state CVIEW system sends a vehicle snapshot to the Roadside Operations system.

ETE–05: Carrier Renews IRP Credential

General Data Flow:
1. The CV Administration sends a renewal reminder to the carrier.
2. The carrier submits the IRP Renewal Application to the CV Administration.
3. The CV Administration performs status checks as required for the state IRP business processes.
4. If the application is approved, the CV Administration sends an invoice notice back to the carrier.
5. The carrier receives the invoice notice and sends payment information.
6. The CV Administration receives payment information and sends the IRP credential to the carrier.
7. The CV Administration sends a vehicle snapshot update to the state CVIEW system.
8. The state CVIEW system sends a T0022 IRP Registration (Cab Card) Input Transaction to the SAFER system.
9. The state CVIEW system sends a vehicle snapshot to the Roadside Operations system.

ETE–06: Carrier Renews IFTA Credential

General Data Flow:
1. The CV Administration sends a renewal reminder to the carrier.
2. The carrier submits the IFTA Renewal Application to the CV Administration.
3. If applicable, the CV Administration may query the IFTA Clearinghouse for the carrier's account status.
4. If applicable, the IFTA Clearinghouse sends the status back to the CV Administration.
5. If the application is approved, the CV Administration sends an invoice notice back to the carrier.
6. The carrier receives the invoice notice and sends payment information.
7. The CV Administration receives payment information and sends the credential to the carrier.
8. The CV Administration sends a snapshot update to the state CVIEW system.
9. The state CVIEW system sends a T0019 IFTA Input Transaction to the SAFER system.
10. The state CVIEW system sends the updated snapshot to the Roadside Operations system.
11. ASPEN queries CVIEW or SAFER for the carrier snapshot, which should reflect the snapshot updates.

ETE–11: Carrier Adds More Than One Vehicle (IRP Supplemental)

General Data Flow:
1. The carrier submits an IRP Supplemental Application for adding one vehicle in one weight group and two vehicles in another weight group.
2. The CV administration performs status checks as required for the state IRP business processes.
3. If the application is approved, the CV Administration sends an invoice notice back to the carrier.
4. The carrier receives the invoice notice and sends payment information.
5. The CV Administration receives payment information and sends the credentials for the vehicles to the carrier.
6. The CV Administration sends a vehicle snapshot update to the state CVIEW system.
7. The state CVIEW system sends a T0022 IRP Registration (Cab Card) Input Transaction to the SAFER system.
8. The state CVIEW system sends a vehicle snapshot to the Roadside Operations system.

WETE–01: Carrier Adds Vehicle (IRP Supplemental)

General Data Flow:
1. The carrier submits an IRP Supplemental Application for adding a vehicle via an Internet browser to the state Web site.
2. The CV Administration performs status checks as required for the state IRP business processes.
3. If the application is approved, the CV Administration sends an invoice notice back to the carrier via the Web site.
4. The carrier receives the invoice notice and sends payment information via the Web site.
5. The CV Administration receives payment information and sends the credential to the carrier via the Web site.
6. The CV Administration sends a vehicle snapshot update to the state CVIEW system.
7. The state CVIEW system sends a T0022 IRP Registration (Cab Card) Input Transaction to the SAFER system.
8. The state CVIEW system sends a vehicle snapshot to the Roadside Operations system.

WETE–04: Carrier Adds Jurisdiction (IRP Supplemental)

General Data Flow:
1. The carrier submits an IRP Supplemental Application for adding a jurisdiction via an Internet browser to the state Web site.
2. The CV Administration performs status checks as required for the state IRP business processes.
3. If the application is approved, the CV Administration sends an invoice notice back to the carrier via the Web site.
4. The carrier receives the invoice notice and sends payment information via the Web site.
5. The CV Administration receives payment information and sends a credential to the carrier via the Web site.
6. The CV Administration sends a snapshot update to the state CVIEW system.
7. The state CVIEW system sends a T0022 IRP Registration (Cab Card) Input Transaction to the SAFER system.
8. The state CVIEW system sends a vehicle snapshot to the Roadside Operations system.

WETE–05: Carrier Renews IRP Credential

General Data Flow:
1. The CV Administration sends a renewal reminder to the carrier.
2. The carrier submits the IRP Renewal Application via an Internet browser to the state Web site.
3. The CV Administration performs status checks as required for the state IRP business processes.
4. If the application is approved, the CV Administration sends an invoice notice back to the carrier via the Web site.
5. The carrier receives the invoice notice and sends payment information via the Web site.
6. The CV Administration receives payment information and sends the IRP credential via the Web site.
7. The CV Administration sends a vehicle snapshot update to the state CVIEW system.
8. The state CVIEW system sends a T0022 IRP Registration (Cab Card) Input Transaction to the SAFER system.
9. The state CVIEW system sends a vehicle snapshot to the Roadside Operations system.

WETE–06: Carrier Renews IFTA Credential

General Data Flow:
1. The CV Administration sends a renewal reminder to the carrier.
2. The carrier submits the IFTA Renewal Application via an Internet browser to the state Web site.
3. If applicable, the CV Administration may query the IFTA Clearinghouse for the carrier's account status.
4. If applicable, the IFTA Clearinghouse sends the status back to the CV Administration.
5. If the application is approved, the CV Administration sends an invoice notice back to the carrier via the Web site.
6. The carrier receives the invoice notice and sends payment information via the state Web site.
7. The CV Administration receives payment information and sends the credential to the carrier via the Web site.
8. The CV Administration sends a snapshot update to the state CVIEW system.
9. The state CVIEW system sends a T0019 IFTA Input Transaction to the SAFER system.
10. The state CVIEW system sends the updated snapshot to the Roadside Operations system.
11. ASPEN queries CVIEW or SAFER for the carrier snapshot, which should reflect the snapshot updates.

WETE–11: Carrier Adds More Than One Vehicle (IRP Supplemental)

General Data Flow:
1. The carrier submits an IRP Supplemental Application for adding one vehicle in one weight group and two vehicles in another weight group via an Internet browser to the state Web site.
2. The CV administration performs status checks as required for the state IRP business processes.
3. If the application is approved, the CV Administration sends an invoice notice back to the carrier.
4. The carrier receives the invoice notice and sends payment information via the state Web site.
5. The CV Administration receives payment information and sends the credentials for the vehicles to the carrier via the Web site.
6. The CV Administration sends a vehicle snapshot update to the state CVIEW system.
7. The state CVIEW system sends a T0022 IRP Registration (Cab Card) Input Transaction to the SAFER system.
8. The state CVIEW system sends a vehicle snapshot to the Roadside Operations system.

APPENDIX C. CHANGE REQUESTS (CRS) INCORPORATED INTO THE CURRENT VERSION

The effect of each CR incorporated into Version 4.0 of the document is briefly described below.

CR 5678 – Update *COACH Part 1*

Changes to the wording were implemented to simplify the text and increase readability. Other types of changes made are noted below:

- Change all references to JHU/APL CVISN Web site to FMCSA CVISN Web site;
- Update document point of contact;
- Delete note referring to the Motor Carrier Safety Improvement Act;
- Delete summary of changes at the beginning of the document;
- Delete hyperlinks that do not work;
- Delete Figure 1-1 “The COACH Supports the Workshops” and references to workshops;
- Delete Figure 1-2 “CVISN System Design – Stakeholder View”;
- Section 1.3 in the old version, “How States Should Use This Document”, becomes Section 1.4 in this version;
- Change “state” to “jurisdiction” in all statements regarding IRP and IFTA agreements;
- Add summary of Core CVISN requirements in Section 1.3;
- Delete material on EDI, CAT, and outdated safety systems;
- In Chapter 4 tables, change “Req Level” from “Req Level (L1/E/C)” to “Req Level (Core/Expanded)” with values
  - (Core) This rating identifies a Core CVISN compatibility requirement.
  - (Expanded) This rating indicates an Expanded CVISN capability that a Core CVISN compliant state may choose to implement.
- Delete CR numbers from the tables in Chapter 4;
- In Chapter 4, shade cells in tables where user is not supposed to enter a value;
- In Chapter 4.3, deleted “ [Single State Registration System (SSRS)]”;

- In Chapter 4.3, delete the text:
  - FMCSA encourages the exploration of XML as an alternative to EDI for computer-to-computer interfaces between carriers and states.

    This is a policy regarding Core CVISN. If a state chooses to first implement a Web-based (person-to-computer) credentialing approach, then implementation of a computer-to-computer interface is considered an Enhanced capability. Similarly, if a state first chooses to implement a computer-to-computer credentialing approach, then implementation of a Web-based interface is considered an Enhanced capability.
- In Table 4.4.1, add the concept: "Electronic screening is provided using license plate readers or technology other than DSRC transponders";
- Add new Chapter 5, "Data Maintenance Requirements", which was previously in *COACH Part 3*;
- Delete references to documents that are going to be/have been archived;
- Delete following references:
  - ASTM Standard E2158-01, Standard Specification for Dedicated Short Range Communication (DSRC) Physical Layer Using Microwave in the 902 to 928 MHz Band, September 2002.
  - ASTM, PS105-99 Standard Provisional Specification for Dedicated Short-Range Communication (DSRC) Data Link Layer, June 2000.
  - IEEE Standard 1455-99, Standard for Message Sets for Vehicle/Roadside Communications, September 1999.
  - The U. S. Department of Transportation, Federal Highway Administration, *Proposed Rule: Dedicated Short Range Communications In Intelligent Transportation Systems (ITS) Commercial Vehicle Operations*, 23 CFR Part 945, [FHWA Docket No. FHWA 99-5844] RIN 2125-AE63, published in Federal Register: December 30, 1999 (Volume 64, Number 250)], Page 73674-73742. Available from the Federal Register Online via GPO Access, http://www.access.gpo.gov/su_docs/aces/aces140.html [DOCID:fr30de99-43].
- Add following references:
  - John A. Volpe National Transportation Systems Center (Volpe Center), *Safety and Fitness Electronic Records (SAFER) Interface Certification Procedure (ICP)* Version 1.0, July 2003. The latest version will be available on the Federal Motor Carrier Safety Administration (FMCSA) CVISN Web site.
  - Volpe Center, *SAFER Commercial Vehicle Information Exchange Window (CVIEW) Interface Re-Certification*, v7, January 2008. The latest version will be available on the Federal Motor Carrier Safety Administration (FMCSA) CVISN Web site.

  - Volpe Center, *SAFER CVISN State Data Baseline Procedure*, Version 1.0, March 2008. The latest version will be available on the Federal Motor Carrier Safety Administration (FMCSA) CVISN Web site.
  - JHU/APL, *Commercial Vehicle Information Systems and Networks (CVISN) Architecture [Revised]*, POR-02-7364 V3.0, December 2006. The latest version will be available on the Federal Motor Carrier Safety Administration (FMCSA) CVISN Web site.
  - Volpe Center, *SAFER Interface Control Document*, Version 8.1, March 2008. The latest version will be available on the Federal Motor Carrier Safety Administration (FMCSA) CVISN Web site.
- Delete Appendix B "Change Requests (CRs) Incorporated into Previous Versions";
- Add new Appendix B "Recommended End-to-End Tests";
- Delete references to CRs that were addressed in the previous version of the document;
- Delete references to SSRS;
- Change references to "CVISN Level 1" to "Core CVISN";
- Change references to "Enhanced CVISN" to "Expanded CVISN";
- Change column "Recommended Interoperability Tests for Technical Deployment" in Appendix A checklists to "Comments";
- Delete column with pairwise tests from tables in Appendix A.

CR 5692 – Update COACH Part 1 – Deleted/Modified Requirements and Changed Criteria

These requirements have been deleted:

- In Table 4.3-2, delete requirement 4.3.23:
  Provide revoked IFTA motor carrier information to other jurisdictions via State On-line Enforcement System (STOLEN).
- In Table 4.4-2, delete subcriteria 2, 2a, 2b, and 2c under requirement 4.4.1, because the rulemaking was withdrawn:
  Be prepared to transition to the sandwich specification after rulemaking is complete. [See the Notice of Proposed Rulemaking (NPRM) regarding DSRC in ITS CVO.]

These concepts/requirements have been modified:

- In Table 4.1-1, item #10, change "ANSI ASC X12 EDI transactions are used for some carrier-state information systems' interactions. XML will be also used in the future" to "HTML/XML are used for most carrier-state information systems' interactions";
- In Table 4.2-2, change requirement 4.2.1 item #6 to "To assist in inspection, use DSRC or other available technologies to retrieve summary vehicle safety sensor data, if driver allows and vehicle is properly equipped."
- In Table 4.2-2, change requirement 4.2.1 item #7 to "To assist in inspection, use DSRC or other available technologies to retrieve driver's daily log, if driver allows and vehicle is properly equipped."
- In Table 4.2-2, add subcriteria under requirement 4.2.9 regarding implementing CVIEW.

These criteria have been modified:

- In Table 4.2-2, requirement 4.2.1, change verification approach from "D" to "T/D";
- In Table 4.3-2, requirements 4.3.1, 4.3.7, and 4.3.10, delete the subcriteria.
- In Table 4.3-2, requirements 4.3.7 and 4.3.10, change verification approach from "T" to "T/D".