
# ITD Core Compliance Monitoring Plan

**Version 3.0**

**May 2019**

Prepared for

US Department of Transportation
Federal Motor Carrier Safety
Administration

1200 New Jersey Avenue,
SE Washington, DC 20590

# Contents


1 Introduction ..... 1

2 Purpose of this Document ..... 2

3 ITD Core Compliance Requirements ..... 2

3.1 Safety Information Exchange ..... 2

3.2 Electronic Credentials Administration ..... 2

3.3 Electronic Screening ..... 3

3.4 Data Quality ..... 3

4 ITD Core Compliance Monitoring Program ..... 3

4.1 Core Compliance Review Purpose and Objectives ..... 3

4.2 Core Compliance Review Overview ..... 3

5 Core Compliance Review and Improvement Process ..... 4

5.1 Selecting States for Review ..... 4

5.1.1 Selection Criteria ..... 4

5.1.2 Review and Approval of Selected States ..... 5

5.1.3 Scheduling State Reviews ..... 5

5.2 Conducting the State Review ..... 5

5.2.1 Kick-off Meeting ..... 5

5.2.2 Core Compliance Review Checklists ..... 5

5.4 Review Results and Recommendations ..... 11

5.5 State Response and Performance Improvement Plan ..... 11

5.6 Review and Approval of State Plans ..... 11

5.7 Monitoring State Progress ..... 11

6 Core Compliance Review Cycle ..... 12

7 State Core Compliance Review Summary ..... 12

# 1 Introduction

The Federal Motor Carrier Safety Administration's (FMCSA) Innovative Technology Deployment (ITD) program was established by the FAST Act on October 1, 2016. The ITD program replaced the Commercial Vehicle Information System and Network program (CVISN), which was established in 1994. ITD supports information sharing involving a partnership of government agencies, motor carriers, and other stakeholders. As such, the ITD program benefits from maximum nationwide participation by public and private partners.

The purpose of the ITD program is to advance the technological capability and promote the deployment of intelligent transportation system (ITS) applications for commercial vehicle operations, including CMV, commercial driver, and carrier-specific information systems and networks. Its goal is a collaborative sharing of the Federal enforcement data and state credentialing data on a national level. With the federal/state information network, States have access to the latest carrier, vehicle and driver information available from SAFER (Safety and Fitness Electronic Records). This access improves the safety and efficiency of the State Commercial Motor Vehicle (CMV) inspection process, utilizing e-screening and other roadside technologies.

The ITD commercial vehicle information systems network is a subset of the National Intelligent Transportation Systems Architecture (ITS); it uses ITS technologies comprising information systems and networks that support commercial vehicle operations. The ITD architecture aligns with the National ITS architecture version 7.0 and includes support for expanded ITD capabilities.

As of December 2017, forty-one States have successfully implemented ITD Core requirements and have been certified by FMCSA. States that are Core compliant are eligible to apply for ITD grant funds to implement expanded ITD functionality.

Even with a formal Core certification process, there are data quality issues that negatively affect the program and hinder participating States' electronic screening processes and their confidence in utilizing CVIEW (Commercial Vehicle Information Exchange Window) data. In response to this issue, both the FMCSA and the ITD stakeholders decided to address data quality as a number one priority at the 2012 CVISN workshop. The Volpe Center was tasked by FMCSA to develop ITD data quality standards, monitor each State's data quality, and provide technical oversight and assistance to help States improve the quality of their data. Volpe has continued this work supporting the ITD Program Office, modifying performance measures in response to the needs of the ITD Program and the ITD Community.

In addition to the data quality issues noted above, other common compliance issues are:

- CVIEW production data does not meet business rules as outlined in the SAFER ICD (Interface Control Document).
- CVIEW interface malfunctions prevent daily data updates from occurring, constrained by limited avenues to connect to the SAFER systems via LAN tunnels.
- ITD States do not apply data requirements in a unified manner.
- ITD States do not send all Core data to SAFER as required.
- ITD States send incorrect data to SAFER.

In order to resolve these issues and improve data quality throughout the program, FMCSA amended its policies, by implementing the Core Compliance Monitoring Program in November 2015. The agency requires ITD States to maintain Core compliance after their initial Core certification.

# 2 Purpose of this Document

This document describes the ITD Core Compliance Monitoring Program (CCMP). It summarizes the ITD Core compliance requirements, and outlines the State Core Compliance Review (CCR) process. FMCSA plans to review the Core compliance of approximately six to eight States annually. The procedures contained herein are organized by critical steps in the CCR process.

The intended audience for this document includes FMCSA, ITD States, and the ITD Support team at the Volpe Center. The document assumes the reader has a familiarity with the ITD Program and any Core compliance requirements.

# 3 ITD Core Compliance Requirements

According to the COACH (V6, March 2014), a State is considered Core compliant if it meets the following criteria:

- Has an organizational framework for cooperative system development established among State agencies and motor carriers.
- Has an established ITD system design that conforms to the latest ITD Architecture and can evolve to include new technologies and capabilities.
- Can meet the requirements of the following three ITD capability areas: Safety Information Exchange, Electronic Credentials Administration, and Electronic Screening.

In addition, in 2014, FMCSA added Data Quality to the Program policy as an enhanced requirement.

## 3.1 Safety Information Exchange

- Inspection reporting using ASPEN (or equivalent) at all major inspection sites. Inspection data sent to SAFER (Safety and Fitness Electronic Records) directly or indirectly.
- Connection to the SAFER system to provide the exchange of interstate carrier and vehicle data snapshots among States.
- Implementation of Commercial Vehicle Information Exchange Window (CVIEW) system (or CVIEW equivalent) to store intrastate data and deliver interstate data to SAFER.

## 3.2 Electronic 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 fuel 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 percent of the IRP and IFTA transaction volume handled electronically; ready to bring on more carriers as carriers sign up; ready to extend to branch offices where applicable.

### 3.3 Electronic Screening

- State uses snapshots to support screening decisions.
- State has implemented e-screening at a minimum of one fixed or mobile inspection site.
- State is ready to replicate e-screening at other sites.

### 3.4 Data Quality

- Core ITD States are responsible for sending complete, accurate, and valid data to SAFER.
- Beginning in FY 2015, FMCSA formally accepted State grant applications for projects to support data quality as a National Priority.
- Core ITD States must maintain a satisfactory level of data quality performance.

## 4 ITD Core Compliance Monitoring Program

On September 14, 2015, the FMCSA Program Manager announced the development and implementation of the Core Compliance Monitoring Program (CCMP). The objective of this program is to ensure that States maintain their Core compliance before being considered for future grant awards. To achieve this objective, FMCSA plans to review the Core Compliance status of approximately six to eight States annually. Each CCR will focus primarily on ITD data quality, State system operations, ITD programmatic requirements, and technical challenges.

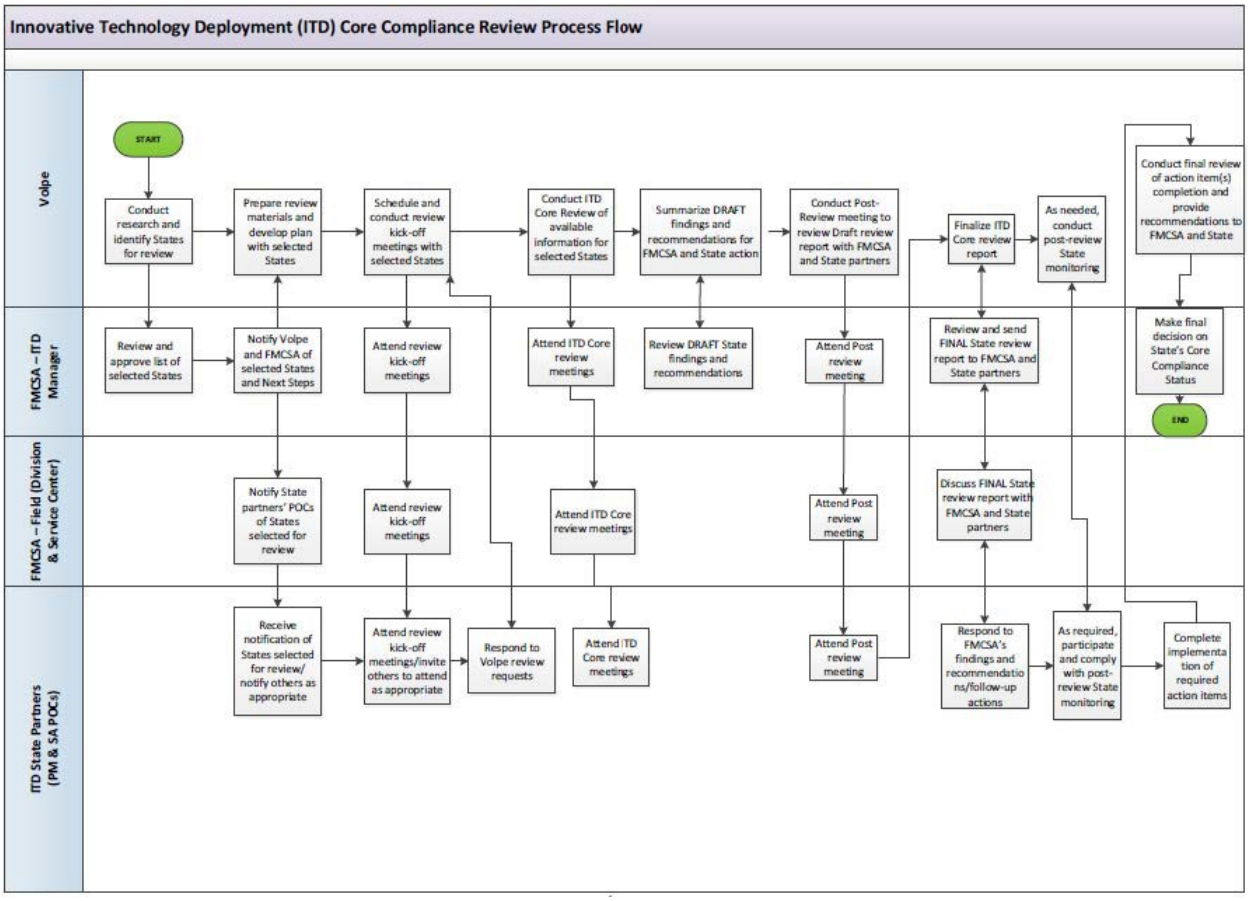
### 4.1 Core Compliance Review Purpose and Objectives

The purpose of the CCR is to monitor ongoing compliance with the Core ITD requirements to ensure that the State has remained Core Compliant since its initial certification. The objective is to observe and assess the strength and weakness in a State's ITD operation, and to develop strategic advice and recommendations for improvement. The ultimate goal of Core compliance review and monitoring is to safeguard ITD data quality and therefore to protect the integrity of the ITD Program.

### 4.2 Core Compliance Review Overview

The high-level steps of the CCR process include:

- Identify States for CCR.
- Communicate with each selected State to establish a time table for review.
- Conduct CCR of each selected State.
- Present review observations and findings to the State; discuss recommendations, actions, and desired timeline for improvement.
- State responds with its plan to address the FMCSA recommendations.
- FMCSA reviews and approves the State's plan and monitors progress through completion. The CCR process flow is illustrated below.




# 5 Core Compliance Review and Improvement Process

## 5.1 Selecting States for Review

During the first quarter of the fiscal year, the Volpe ITD support team will evaluate the overall performance of ITD States, identify potential candidates for a CCR, and submit a candidate list to FMCSA for approval.

### 5.1.1 Selection Criteria

State selection will be based on the following criteria:

- Trending issues in the ITD Data Quality Performance Reports.
- Satisfactory Data Quality rating (≥ 2.5).
- Technical or programmatic challenges:
  - State vendor transition
  - State ITD program resource issues
  - State infrastructure and/or network changes
  - State system design changes
  - Production operational and maintenance issues.
- Communication issues with the ITD support team.
- Core certification status for one year or more.
- Core compliance has lapsed, but the State has not been formally de-certified.
- Geographical representation with a minimum of one State from each FMCSA Service Center.

### 5.1.2 Review and Approval of Selected States

- The FMCSA ITD Program Manager will review the ITD Support team's list of recommended States and make the final decision on selection.
- The FMCSA ITD Program Manager will notify the ITD Support team and the FMCSA Division Offices of the selected States and next steps.
- The ITD Support Team will prepare review material and develop a plan with each selected State.
- The FMCSA ITD Program Manager, through the FMCSA Division Offices, will notify State partners of upcoming reviews.

### 5.1.3 Scheduling State Reviews

Upon FMCSA's approval of the selected States, the ITD support team will contact State ITD Program Managers to schedule review appointments that are mutually acceptable. The CCRs will be conducted between December and September each year. When scheduling, the ITD Support team will discuss with the State whether the review will be conducted remotely or onsite, and then coordinate the next steps.

## 5.2 Conducting the State Review

### 5.2.1 Kick-off Meeting

Each State CCR will start with a kick-off meeting conducted remotely via web meeting and conference call. The FMCSA ITD Program Manager, FMCSA Division Office staff, the ITD support team, and the State ITD Manager and technical leads must attend the kick-off meeting to discuss the purpose of the review, the roles and responsibilities of personnel, the CCR process, logistics for the review, and post-review activities and outcomes.

### 5.2.2 Core Compliance Review Checklists

Comprehensive checklists have been developed for conducting the CCR based on Core compliance requirements in the following four program areas: Data Quality Performance Measures, Certification and Recertification, Production Operation, and Programmatic Requirements.

## A. Data Quality Performance Measures

The data quality checklist will be used to review States current performance and adherence to the data standards of the ITD program.

| A. Data Quality Performance Measures | | |
|---|---|---|
| **ITD Program Area** | **ITD Requirement/Standard** | **Rating** |
| **1. Data Quality Measurements (T-22 IRP)** | | |
| | **a.** M1 – State uploads new and updated records to SAFER within 24 hours. | |
| | **b.** M2 – State data complies with XML schema and data definitions. | |
| | **c.** M3 – State correctly uses the date last updated by the State. Last Update Date to indicate if the data uploaded is the most recent data. | |
| | **d.** M4 – State's IRP registration data has valid vehicle status codes that match the vehicle registration status. | |
| | **e.** M5 – State sends IRP baseline data to SAFER at least once every 12 months. | |
| **2. Data Quality Measurements (T-19 IFTA)** | | |
| | **a.** M1 – State uploads new and updated records to SAFER within 24 hours. | |
| | **b.** M2 – State data complies with XML schema and data definitions. | |
| | **c.** M3 – State uses the Last Update Date to indicate whether the data uploaded is the most recent data. | |
| | **d.** M4 – State provides valid IFTA status code that matches the IFTA account status. | |
| | **e.** M5 – State sends IFTA baseline data to SAFER at least once every 12 months. | |
| **3. Data Quality Issue Responsiveness** | | |
| | **a.** State responds to data quality (DQ) issues within 30 days. | |
| | **b.** State resolves data quality issues within 90 days. | |

## B. Certification and Recertification

After initial certification, States must maintain the technical compliance of the SAFER/CVIEW interface in production. The State must be recertified after major network, server, or application changes; after switching to a new vendor's support; when the SAFER/CVIEW interface changes; or after remediation of major data quality issues. This checklist is used to review the State's level of communication with the ITD support team regarding these conditions and recertification requirements.

| B. Certification and Recertification | | |
|---|---|---|
| **ITD Program Areas** | **ITD Requirement/Standard** | **Rating** |
| **1. Certification** | | |
| | **a.** State safeguards its original FMCSA certification letter for all certified data exchange transactions. | |
| **2. Recertification** | | |
| | **a.** State communicates with ITD support team for recertification after major changes in network, server and application. If any interface system is changed, the certification tests are re-run as part of the recertification process. | |
| | **b.** State communicates with ITD support team for recertification after switching to a new vendor's support. If any interface system is changed, the certification tests are re-run as part of the re-certification process. | |
| | **c.** State communicates with ITD support team for recertification when SAFER/CVIEW interface changes. If any interface is changed, the certification tests are re-run as part of the recertification process. | |
| | **d.** State communicates with ITD support team for recertification after remediation of major data quality issues. If any interface system is changed, the certification tests are re-run as part of the recertification process. | |

## C. Production Operation

States must conform to the ITD business requirements in production. This checklist is used to review the State's routine operational procedures.

| C. Production Operations | | |
|---|---|---|
| **ITD Program Areas** | **ITD Requirement/Standard** | **Rating** |
| **1. Production Operation** | | |
| | **a.** State has a daily routine to monitor CVIEW uploads and downloads. | |
| | **b**. State checks SAFER processing logs on daily basis. | |
| | **c.** State applies business rules correctly in selecting carrier and vehicle data to send to SAFER. | |
| **2. Electronic Credential Information Exchange** | | |
| | a. State can document that at least 10% of IFTA transactions are handled electronically. | |
| | b. State can document that at least 10% of IRP transactions are handled electronically. | |
| | c. State has connections to IFTA Clearinghouse. | |
| | d. State has connections to IRP Clearinghouse. | |
| | e. State has implemented other credentials – titling, HazMat, and oversize/overweigh (OS/OW). | |
| | f. State updates CVIEW with intrastate and interstate data in timely manner. | |
| | g. State's CVIEW uploads interstate data to SAFER within 24 hours. | |
| **3. Safety Information Exchange** | | |
| | **a.** State sends inspection data to SAFER using Aspen or equivalent. | |
| | **b.** State's CVIEW (or equivalent) facilitates exchange of intrastate and interstate carrier and vehicle data within the State. | |
| | **c.** State's CVIEW (or equivalent) uploads interstate carrier and vehicle data to SAFER through snapshots. | |
| **4. Electronic Screening** | | |
| | **a.** State uses safety data from SAFER snapshots to support screening decisions. | |
| | **b.** State uses credentialing data from SAFER snapshots to support screening decisions. | |

| C. Production Operations | | |
|---|---|---|
| **ITD Program Areas** | **ITD Requirement/Standard** | **Rating** |
| | **c.** State has implemented a minimum of one fixed or mobile inspection site. Ready to replicate at other sites. | |
| | **d.** State uses Weigh-In-Motion (WIM) at mainline speed or on the ramp, or weight history in making screening decisions. | |
| | **e.** State is a member of NORPASS, PrePass™ or DriveWyze. If not, demonstration or inspection of State system design documents. Share vehicle information with other jurisdictions. | |
| **5. System Design** | | |
| | **a.** State CVIEW is configured with State source systems to receive timely updates of core records so that the State CVIEW system has the complete set of records for safety, credential, and e-screening. | |
| | **b.** State CVIEW has the mechanism to identify the data that must be sent to SAFER within 24 hours. | |
| | **c.** State demonstrates its system design conforms to the ITD architecture – whether it sends data directly to SAFER or via State vendor systems. | |

## D. Programmatic Requirements

State ITD Program Managers are responsible for the overall development and maintenance of their State's ITD implementation. The Programmatic Requirements checklist is used to review a Program Manager's participation and supervision of daily operations of the ITD program. The Program Manager is also required to provide guidance and oversight to program vendor(s) to ensure that vendor support is sound and fulfills the State's requirements. *In FY19, the ITD grant program management review was added as a new area in checklist D.*

| **D. Programmatic Requirements** | | |
|---|---|---|
| **ITD Program Areas** | **ITD Requirement/Standard** | **Rating** |
| **1. ITD Program Management** | | |
| | **a.** State ITD program manager attends monthly Program Manager call/webinar. | |
| | **b.** State has at least one representative attend monthly ACCB call/webinar. | |
| | **c.** State submits quarterly reports on its ITD operations per the established schedule. | |
| | **d.** State ITD manager reviews and shares monthly ITD Data Quality report. | |
| | **e.** State keeps its Program Plan/Top Level Design (PP/TLD) up to date (at minimum, updates every 5 years). | |
| | **f.** State's designated ITD lead agency coordinates with other State agencies on project funding and resources. | |
| | **g.** Lead agency coordinates with other organizations in the State for SAFER/CVIEW connections and data sharing | |
| **2. Contractor Management** | | |
| | **a.** State ITD program manager reviews the State's vendor performance periodically. | |
| **3. Communications** | | |
| | **a.** State proactively provides updates to FMCSA and its ITD support team on changes to ITD POC, vendor support, network connection, hosting service, and when there are issues with production operation, project delays, funding lapses, etc. | |
| **4. ITD Grant Program Management** | | |
| | a. State effectively manages all open ITD grant awards. | |
| | b. State manages available grant funds within period of performance. | |
| | c. State monitors all project milestones to ensure completion. | |
| | d. State provides timely grant quarterly reports as required. | |

## 5.4 Review Results and Recommendations

The process for developing and finalizing review results and recommendations includes the following:

- Upon completion of the onsite or remote review, the ITD support team will summarize findings and recommendations in a report for FMCSA's review and approval.
- The ITD support team will schedule a follow-up meeting to present and discuss the review results and their recommendations, along with the relevant ITD Core requirements, with the State. The ITD team will explain the expected response from the State, and the programmatic consequences if the State fails to comply. Typically, such meetings will be conducted two to six weeks after the review, with scheduling subject to availability of requested parties.
- After the follow-up meeting, the ITD team will finalize the report, incorporating new information or acknowledging the State's comments as appropriate. FMCSA ITD program manager will distribute the report to the FMCSA Division Office, Service Center and the State ITD program leads.

Additionally, FMCSA will review ITD Core compliance requirements, the expected outcome from the State, and the programmatic consequences if the State fails to comply. Failure to maintain Core

Compliance standards may jeopardize a State's future grant funding and /or Core compliance status.

## 5.5 State Response and Performance Improvement Plan

States must submit their responses to FMCSA's findings and recommendations within 30 days of receiving the final review report. The State's response must provide their plan, with timelines, to maintain Core compliance. Specifically:

- If the State has satisfactory review ratings, it should continue maintaining their Core compliance status. No further action is required.
- If the State has any identified operational issues, it must address each of those issues with a planned timeline for resolution. A State's plan must also include a methodology to maintain Core compliance.

## 5.6 Review and Approval of State Plans

Upon receiving the State's responses and plan for improvement, the FMCSA Program Office will review for acceptance and supply feedback, clarification, and suggestions to the State in a timely manner. The State will have an opportunity to modify their plan if deemed necessary. The final approved plan, together with the State CCR report, will be archived by FMCSA.

## 5.7 Monitoring State Progress

The FMCSA Program Office ITD Support team will work closely with each State to provide technical assistance and monitor progress against the State's plan. When needed, the ITD support team will conduct a 'mini review' to ensure that a State is on track to implement their corrections. The following list identifies the post-review activities to be performed by the FMCSA ITD support team and the State:

- ITD Support team to schedule a 3-month post-review check-in.
- ITD Support team to schedule a 6-month post-review check-in.
- ITD Support team to support any technical issues that arise on the State's side.
- State to provide quarterly status update on tasks in their plan.

The ITD Support team will report to FMCSA when a State has successfully implemented their planned projects for Core Compliance. FMCSA will review the recommendations from the ITD Support team and approve the review closure when the performance is satisfactory. The review closure criteria include but are not limited to:

- Satisfactory rating from post-review check-ins.
- No outstanding operational issues observed by the ITD Support team.
- Overall Data Quality Measure Rating is ≥ 2.5.
- Responses to reported data quality issues are timely with no issues outstanding for more than one month.

# 6 Core Compliance Review Cycle

Under normal circumstances, a State will be selected for review once every 5-6 years. If a State encounters unusual challenges that could impact its performance, an interim review will be conducted to ensure that the State's Core compliance status is not compromised.

# 7 State Core Compliance Review Summary

State:___State POC Name: State POC Phone: ( )