

SAFER Interface Certification Procedures

Version 1.0

28 July 2003

Prepared by:

The Volpe National Transportation Systems Center
Surface Transportation Information Systems Division (DTS-26)
Cambridge, MA

Prepared for:

Federal Motor Carrier Safety Administration (FMCSA)

Table of Contents

1	Introduction	1-1
1.1	Purpose	1-1
1.2	Scope	1-1
2	Connectivity Requirements	2-1
2.1	Introduction.....	2-1
3	Testing Schedule	3-1
4	Data Requirements	4-1
4.1	Introduction.....	4-1
4.2	XML / FTP Interface	4-1
4.3	Transactions and Interface Identification.....	4-1
4.4	Data Maintenance Requirements	4-1
5	Testing Procedures	5-3
5.1	Introduction.....	5-3
5.2	Verify Connectivity	5-3
5.3	Detailed Testing Procedures	5-3
6	State Certification Matrix.....	6-1

1 Introduction

1.1 Purpose

This document specifies the procedures to be completed to certify that communications and data exchange mechanisms between state Commercial Vehicle Information Exchange Window (CVIEW) systems and the Federal Motor Carrier Safety Administration's (FMCSA) Safety and Fitness Electronic Records (SAFER) system hosted at the Volpe National Transportation systems Center (Volpe Center) are in compliance with all applicable SAFER interface and security requirements to ensure the accuracy and quality of the data exchanged, efficient communications, and the prevention of system corruption or performance degradation. Certification is required before a state CVIEW system will be allowed to connect to the production version of SAFER.

The procedures contained herein are generally organized following the order of transaction detail descriptions contained in the SAFER v4.2 Interface Control Document, Version 1.0 (ICD) that can be found at the FMCSA CVISN Program web site (<http://www.jhuapl.edu/cvisn>).

The intended audience for this document includes state Commercial Vehicle Information System and Network (CVISN) Architects, system developers, and contractors responsible for the implementation of CVIEW systems within their state. The document assumes the reader has a familiarity with XML processing and, in particular, the ICD.

1.2 Scope

This document focuses on the certification requirements and procedures for the interface of CVIEW systems to SAFER using the Extensible Markup Language (XML) transaction features of SAFER Version 4.2. Follow-on changes to this document will address specific certification requirements and procedures for certification of SAFER Electronic Data Interchange (EDI) transactions.

For purposes of this document, "CVIEW systems" are defined to include systems designed to exchange motor carrier safety data with the SAFER system in accordance with the requirements of the FMCSA CVISN program.

In general, the tests and procedures contained herein will require the state to demonstrate accurate, efficient, and secure:

1. Connectivity to the Volpe Center network segment hosting the SAFER system,
2. Downloading and processing XML Output transactions from SAFER to their CVIEW system, and
3. Uploading and processing XML Input transactions from their CVIEW system to SAFER.

Upon successful completion of the above, the Volpe Center will submit a request to the FMCSA for approval of the CVIEW 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.

Certification will be for the download and processing of all SAFER XML output transactions, but for only specific XML input transactions for which the CVIEW system has successfully completed the test procedures. If, at a later date, the state desires to certify their CVIEW system for additional XML input transactions, certification for those specific transactions must be completed in accordance with this document. In addition, re-certification will be required when new types of SAFER input XML transactions become available and/or substantial changes to existing transactions or systems are implemented by the state, as determined by the FMCSA. Compliance with this policy will be enforced initially through a manual inspection process that will eventually be automated.

The testing procedures and exercises will focus on testing each of the CVIEW transaction processes outlined in the ICD. Each process will receive specially designed input data files developed to test the accurate, efficient and secure implementation of that transaction type on the CVIEW system. In addition states will be required to provide details of their own locally developed data to be used for the testing of CVIEW processing and XML transaction creation. Test data XML transaction files should contain multiple records, up to the limit specified in the ICD. Additionally states are encouraged to use as many optional fields as possible.

States failing specific transaction testing will be allowed to re-schedule and re-test for certification for those transactions. Re-scheduling will take into consideration other state certifications scheduled and the availability of the Volpe Center staff and resources.

2 Connectivity Requirements

2.1 Introduction

CVIEW has been designed to exchange, i.e. upload and download, carrier snapshot and registration information with the Safety and Fitness Electronic Records (SAFER) system via the FMCSA File Transfer Protocol (FTP) server system housed at the Volpe Center. SAFER (as well as other FMCSA IT Systems) is “housed” within a secure computer center and network environment at the Volpe Center in Cambridge, Massachusetts. The system is protected and isolated from the Internet by an appropriately designed firewall system. CVIEW states can connect to the SAFER system in the following ways:

- Via AAMVAnet Frame Relay, a non-Internet-based, LAN-to-LAN permanent connection. AAMVAnet is considered a “trusted” network provider for FMCSA systems housed at the Volpe Center. This method establishes a permanent virtual circuit (PVC) from the user’s LAN to the Volpe Center. The AAMVAnet point of contact for establishing a Frame Relay, IP based network/Intranet connection to FMCSA IT Systems is Patrice L. Aasmo (paasmo@aamva.org or 703-908-5787).
- Via the Internet, by establishing a persistent virtual private network (VPN) connection from a user’s LAN to the Volpe VPN gateway. This option requires specific equipment compatibility between the Volpe Center and the user’s LAN. For further information on setting up an Internet VPN connection to SAFER, states should contact FMCSA Technical Support at FMCTechSup@volpe.dot.gov.

Any CVIEW state desiring certification will need to have a functioning connection to SAFER via either AAMVAnet or an Internet VPN link in advance of commencing certification testing.

Once connectivity is established, states should contact FMCSA Tech Support, Accounts Management Group, and request CVIEW type accounts for SAFER. These accounts must be in place prior to the certification testing. FMCSA Technical Support can be contacted at (617) 494-5490 or FMCTechSup@Volpe.dot.gov.

3 Testing Schedule

Testing of each state's CVIEW will be conducted sequentially, with no more than one state testing at a time. States should contact Mary Stuart (CVISN Deployment Support) at the Johns Hopkins University/Applied Physics Lab (APL) (Mary.Stuart@jhuapl.edu or 443-778-7001) to advise of their readiness to certify. States should also be prepared to give a fairly firm date on when they would realistically be ready to begin testing. APL will coordinate the testing schedule priority and "queue" with all interested states and FMCSA (MC-RTT) and forward a list of states to the Volpe Center. The Volpe Center will then contact each state individually to finalize testing dates. In the event that re-testing is required by a state, subsequent scheduling will be coordinated through the Volpe Center.

4 Data Requirements

4.1 Introduction

SAFER Version 4.2 supports three external interface types:

1. SMTP/POP3 (e-mail) for the exchange of EDI, ASCII text, and SCAPI AFF formatted files,
2. FTP for the exchange of XML files, and
3. The Remote Procedure Call (RPC) interface.

The following sections briefly define only the FTP interface type.

4.2 XML / FTP Interface

4.2.1 XML / FTP Summary

A CVIEW system will utilize this interface to perform two basic operations: downloading files containing information from various sources including other states, and uploading files containing information to be shared among participating jurisdictions. To accomplish this, the state system will interact with the SAFER system in the manner described in the ICD, Section 4.

4.3 Transactions and Interface Identification

The following transactions are supported by SAFER Version 4.2 through the XML / FTP interface. Collectively, these transactions constitute the SAFER 4.2 XML / FTP transaction set. Each transaction in the transaction set has an identifier (e.g. "T0024" for the Vehicle Transponder ID input transaction) that is unique within the SAFER system. This identifier is used throughout the interface to identify a specific transaction from among those in the transaction set. Only one transaction type per input or output file is allowed.

Note that the table below, which corresponds to the *SAFER Version 4.2 XML/FTP Transaction Set* table in the ICD, has been reorganized to logically group the input transactions with their corresponding output transactions, where applicable. This is a slight change from the table in the ICD which has the transactions listed in numerical order.

Table 4-1. SAFER Version 4.2 XML/FTP Transaction Set

ID	Type	Transaction	Transaction Data Tag
T0019	Input	International Fuel Tax Agreement (IFTA)	IFTA_LICENSE
T0025	Output	International Fuel Tax Agreement (IFTA)	IFTA_LICENSE
T0020	Input	IRP Account	IRP_ACCOUNT
T0026	Output	IRP Account	IRP_ACCOUNT
T0021	Input	IRP Fleet	IRP_FLEET
T0027	Output	IRP Fleet	IRP_FLEET
T0022	Input	IRP Registration (Cab Card)	IRP_REGISTRATION
T0028	Output	IRP Registration (Cab Card)	IRP_REGISTRATION
T0023	Input	Carrier E-Screening Authorization	CARRIER_ESCREEN_AUTHORIZATION
T0024	Input	Vehicle Transponder ID	VEHICLE_TRANSPONDER_ID
T0029	Output	Vehicle Transponder ID	VEHICLE_TRANSPONDER_ID
T0030	Output	Vehicle Inspection Summary	VEHICLE_INSPECTION_SUMMARY
T0031	Output	MCMIS Safety and Census	MCMIS_SAFETY_CENSUS
T0032	Output	Licensing and Insurance	LICENSING_INSURANCE

4.3.1 XML Formats

A SAFER Version 4.2 XML transaction consists of three elements: The interface header, the transaction header, and the transaction information itself. These three XML segments are contained within an over-all transaction root, which is defined via a set of start and end transaction tags, based on the transaction Identification Number (ID) from table 4-1 above. For detailed information on these three elements, please consult the ICD.

4.4 Data Maintenance Requirements

Input Transaction Files:

When SAFER v.4.2 is in production, input transaction files will be deposited by CVIEW in the directory <ftp://ftp.safersys.org/SAFER> utilizing the file naming convention CVIEW<XX><SEQUENCE>.ZIP where

- <XX> is the jurisdiction's two letter postal code, and
- <SEQUENCE> is a 10 character decimal number used to differentiate the file from all others uploaded recently by the jurisdiction.

Note that SAFER will not use the file name to order or prioritize processing. The file naming convention is simply a device to prevent two files having the same name. States are responsible for ensuring their CVIEW systems adhere to the file naming conventions specified in the ICD, in particular the uniqueness of the SEQUENCE. Failure to do so may result in data being overwritten.

Files contained in the directories are compressed utilizing the PK Zip format. See Appendix K of the ICD, Compression Format. The file contained within the zip file should have the same name as the zip file, but with the “.XML” extension.

For examples of these files, please consult the ICD.

Input Transaction Log Files:

The results of processing each input transaction file will be reported in a log file that is made available to CVIEW systems on the SAFER 4.2 FTP server. Each input transaction file has a name that incorporates the sending jurisdiction’s two letter postal code and a sequence indicator (see *Input Transaction Files* above). The log file for a particular input transaction file will have the same file name but use a file extension of “.LOG”. The log files will not be compressed.

The log files corresponding to the input files shown above would be found in the <ftp://ftp.safersys.org/LOGS> directory. For examples of these files, please consult the ICD.

Output Files:

Each output directory will contain a set of transaction baseline files and one or more sets of transaction update files. A baseline set will consist of one or more files that collectively contain all of the information relevant to a particular transaction, as it exists in the SAFER database at the time the baseline set is created. An update file set will consist of one or more files that collectively contain transactions for each change to the SAFER database since the last baseline or update file set was created. Periodically new transaction baseline file sets will be created. Whenever a baseline file set is created, the previous baseline file set will be deleted from the directory as well as all its related subsequent update file sets.

By establishing a local data store using the baseline file set, and then updating the local data store utilizing the update file sets, a state system can keep its database or files completely up to date and in sync with SAFER. Theoretically, by consistently updating the local data store via the update file sets, only one baseline file set need be downloaded during the entire life of the state system. At any time the downloading and processing of the baseline file set and its subsequent update file sets will bring the local CVIEW database into sync with SAFER for that specific transaction set.

Files contained in the output directories are compressed utilizing the PK Zip format. See appendix K of the ICD, Compression Format. The file contained within the zip file should have the same name as the zip file, but with the “.XML” extension.

The files in an XML output transaction directory and in the ZIP file will be named according to the following convention: SAFER<TX>_<Timestamp>.<Content>.<Type>, where

- <TX> is the transaction type (i.e., T0019, T0020, etc.),
- <Timestamp> is the date (in year, month, day format) + time (in 24-hour format, hours, minutes, and seconds)
- <Content> is either “BL” for baseline or “UD” for Update, and

- <Type> is either “ZIP” for compressed archive files in the directory or “XML” for the uncompressed transaction file contained in the zip file.

For examples of these files, please consult the ICD.

5 Testing Procedures

5.1 Introduction

Certification testing consists of two phases that are required for SAFER interface certification, and one phase that supports CVISN interoperability end-to-end tests:

- In Phase One, a manual test will be performed by the state. A set of pre-developed, well-formed test cases will be sent to the states via email, and these test cases will be used to verify both account information and connectivity to the SAFER Certification FTP Server.
- In Phase Two, an automated test will be performed using the state’s CVIEW system. States will be required to provide the Volpe Center details of the data values to be used in the creation and upload of specific transactions. The state CVIEW system is expected to process this data, create an accurate and well-formed XML input transaction, and upload that transaction to the SAFER Certification FTP Server. This test will also prove that the state’s CVIEW system can upload transactions to the proper FTP directory and retrieve and process related output transactions.
- Phase Three provides test data for the state to perform end-to-end interoperability tests by downloading and processing IFTA, IRP, and Vehicle Inspection transactions with flags set to indicate vehicles should be inspected at the roadside. These tests can be performed separately from certification activities and are not required for certification of CVIEW to SAFER data exchange. This test data is being provided to support the CVISN interoperability tests that a state will be required to perform. See the CVISN web site, <http://www.jhuapl.edu/cvisn/>, for more information on CVISN interoperability testing.

5.2 Verify Connectivity

Well in advance of testing, CVIEW states should have implemented a secure connection to SAFER via either AAMVAnet or VPN and requested appropriate user ID’s and passwords. Please see Section 2 for details.

5.3 Detailed Testing Procedures

Please follow the steps below to test your state’s CVIEW transaction processing.

5.3.1 Phase One: Testing Transaction Files via a Manual Process

The testing described in this section will verify the state’s CVIEW account information and will test the connectivity to (both uploading and downloading) the SAFER Certification FTP Server. In this phase, a set of pre-developed, well-formed test cases will be sent to the states via email and the states will use these tests, as described below, to perform the Phase One testing.

5.3.1.1 Log on to the SAFER FTP server using your state’s UserID and Password.

- For users accessing the SAFER Certification FTP server through a web browser, type the following URL into the address bar (without quotes):
 - “ ftp://CVIEWxx:****@ftpcert.safersys.org/ ” where:
 - xx = state ID, i.e., MA, NH,
 - and **** = state password
- For users accessing the SAFER Certification FTP server via FTP, the following will need to be typed at the command line in order to connect to the FTP server (without quotes):
 - “ OPEN [ftpcert.safersys.org](ftp://ftpcert.safersys.org/) ”
 - Once a connection has been established via FTP, the user will be prompted to enter their state UserID and Password.

5.3.1.2 Locate the SAFER directory (this is the directory where the input transaction files will be uploaded).

- If using a web browser, type “SAFER” at the end of the URL in the address bar to access the SAFER directory. The resulting URL will be ftp://CVIEWxx:****@ftpcert.safersys.org/SAFER. After verifying that the correct URL is displayed, press enter.
- If using FTP, use the “CD SAFER” command to get to the SAFER directory. Then verify that you are in the “SAFER” folder using command “PWD”. You would see at the MS-DOS prompt that “/safer” is the current directory.

5.3.1.3 Upload the input transaction files into the SAFER directory, according to the transaction being tested.

- If using a web browser, copy the test file from the state’s local hard drive into the SAFER directory.
- If using FTP, use “PUT” command to put test file into SAFER directory. Please make sure that you first copy the input file to the local hard drive and then “PUT” it in the FTP folder

For testing input transactions T0019, T0020, T0021, T0022, T0023 and T0024, load each test file as described above.

Table 5-1. Input Transaction Load Files

To test input transaction:	User should load file:
T0019	CVIEWxx0000000001.zi p
T0020	CVIEWxx0000000002.zi p

T0021	CVIEW _{xx} 0000000003.zi p
T0022	CVIEW _{xx} 0000000004.zi p
T0023	CVIEW _{xx} 0000000005.zi p
T0024	CVIEW _{xx} 0000000006.zi p

(where xx = state code)

5.3.1.4 Verify the status of the input transaction processing.

- o If using a web browser, navigate to the LOGS directory and double-click on the log file that corresponds to the input transaction file.
- o If using FTP, use “CD LOGS” command to get into the LOGS directory. Then us command to download the correct log file.

Table 5-2. Input Transaction Log Files

Load file:	Log file:
CVIEW _{xx} 0000000001.zi p	CVIEW _{xx} 0000000001.log.xml l
CVIEW _{xx} 0000000002.zi p	CVIEW _{xx} 0000000002.log.xml l
CVIEW _{xx} 0000000003.zi p	CVIEW _{xx} 0000000003.log.xml l
CVIEW _{xx} 0000000004.zi p	CVIEW _{xx} 0000000004.log.xml l
CVIEW _{xx} 0000000005.zi p	CVIEW _{xx} 0000000005.log.xml l
CVIEW _{xx} 0000000006.zi p	CVIEW _{xx} 0000000006.log.xml l

To verify a successful input transaction, check the corresponding log file in the LOGS directory for the status of the transaction.

5.3.1.5 Notify the Volpe Center of Completion of Transaction File Upload

For states ONLY certifying for input transactions, the state will notify the Volpe Center (wu@volpe.dot.gov) that the input test has been completed. The Volpe Center will run a script that will query the database to verify a successful transaction.

5.3.1.6 Locate the desired output transaction directory (these are the directories from where the output transaction files will be downloaded).

If beginning a new session, follow instructions in Section 5.3.1.1 for logging in.

SAFER will generate an output file in the corresponding output transaction directory, according to the table below.

Table 5-3. Transaction Output File Directories

Transaction Description	Input transaction ID	Output transaction directory name (where the output transaction file resides)
IFTA	T0019	T0025
IRP Account	T0020	T0026
IRP Fleet	T0021	T0027
IRP Registration (Cab Card)	T0022	T0028
Carrier E-Screening Authorization & Vehicle Transponder ID	T0023 and T0024	T0029
Vehicle Inspection Summary		T0030*
MCMIS Safety and Census		T0031*
License and Insurance		T0032*

* These transaction files are generated by SAFER directly from the database

- If using a web browser, type the name of the desired output transaction directory (according to Table 5-3) at the end of the URL in the address bar. For example, the resulting URL for an IRP Account transaction will be ftp://CVIEWxx:****@ftpcert.safersys.org/T0026. After verifying that the correct URL is displayed, press enter.
- If using FTP, use the change directory command to get to the desired directory. For example, to access the IRP Account transaction directory, type “CD T0026”. Then verify that you are in the correct folder using command “PWD”. You would see at the MS-DOS prompt that “/T0026” is the current directory.

5.3.1.7 Download the output transaction files to the state’s local hard drive

- If using a web browser, copy the desired output file from the output directory on the SAFER Certification FTP Server to the state’s local hard drive.
- If using FTP, use “GET” command to download the desired output file from the output directory.

5.3.2 Phase Two: Testing Transaction Files via an Automated Process

The objectives of Phase Two testing are to ensure that the CVIEW system is able to generate well-formed, syntactically correct XML input transaction files using their own test data to upload to the SAFER

Certification FTP Server and that CVIEW is able to download and process XML output transaction files from the SAFER Certification FTP Server. In order to properly gauge the success of this test, the state must provide the Volpe Center with the detail data currently residing in their CVIEW system that they plan to include in the uploaded transactions. Note that the state will be responsible for generating the unique transaction file names, so these names will not match the Test Case Names in the attached State Certification Matrix.

5.3.2.1 Upload input transaction data directly from CVIEW system to SAFER

Before starting this phase of the test, states will be required to provide the intended test data to be uploaded from the CVIEW system to the Volpe Center in accordance with the matrix found in the Excel spreadsheet () provided for this purpose. In developing the test data to be used for this phase, XML transaction files should contain multiple records, up to the limit specified in the ICD. Additionally states are encouraged to use as many optional fields as possible. A copy of the *State input data matrix.xls* spreadsheet, if not attached to this document, can be obtained from Jingfei Wu at the Volpe Center (wu@volpe.dot.gov).

Note that the suggested forms provided in the Excel spreadsheet specify the data values needed by the Volpe Center for each transaction being tested to ensure the intended CVIEW data values actually show up in the proper database fields within the SAFER Certification Database. States are welcome to coordinate with Volpe alternate forms and methods of providing this test data in advance of the test.

The CVIEW system should be able to successfully generate the input data files, and send them to the SAFER Certification FTP server, placing them in the SAFER directory.

The state is responsible for the uniqueness of the transaction file names, as the consequences for failing this requirement would be that data would be over written.

5.3.2.2 Verify Update

Upon receiving the notification from the state of completion of the data uploading, the Volpe Center will query the SAFER Certification database to verify that the database has been updated with the information sent from the CVIEW system. The Volpe Center will then enter the results pertaining to the specific test into the State Certification Matrix as required

The Volpe Center will notify the state of the test status.

Should there be any testing failure, the Volpe Center will notify the state and will work together with the state to identify the problem. Once the problem is resolved, the state will initiate another test, repeating this process until the transaction is successful. At least one successful test per transaction is required for the state to be certified.

5.3.2.3 Download output transaction data from the SAFER Certification FTP Server to CVIEW

The Volpe Center will generate baseline file sets and update file sets for every output transaction. These files will be sent to their respective output directories on the SAFER Certification FTP server.

CVIEW systems can either download the baseline files periodically to synchronize their local databases, or simply download updates.

5.3.2.4 Query Local Database

The participating state will use SQL PLUS or equivalent tool to query its local database to obtain record counts for the base tables. This provides a state with a record count before the download.

Example: to get a record count for table carrier

```
SQL> Select count(*) from carrier  
where TO_CHAR(last_update_date, 'YYYYMMDD')=DATE;
```

(DATE=Date and time the CVIEW database is queried.)

5.3.2.5 Download Output Transaction Files

CVIEW system will download the desired output transaction files, process them and update the state's local database.

The state will again query its local database using the query in step 2. The difference of the results of these two queries should equal the total number of records contained in the latest output transaction file. The state will then provide the results to the Volpe Center who will enter the results into the State Certification Matrix.

5.3.2.6 Remediation

Should there be any testing failure, the Volpe Center will notify the state and will work together with the state to identify the problem. Once the problem is resolved, the state will initiate another test, repeating this process until the transaction is successful. At least one successful test per transaction is required for the state to be certified.

5.3.2.7 Complete Testing for All Output Transactions

The state will complete testing for all output transactions the state would like to be certified for, and notify the Volpe Center of their results, which will be entered into the State Certification Matrix.

5.3.2.8 Completed State Certification Matrix

The Volpe Center will review the results contained in the State Certification Matrix, then submit a request for certification to FMCSA (MC-RIS).

5.3.3 Phase Three: Support for State End-to-End Interoperability Testing

The objective of Phase Three is to provide test data for the state to perform end-to-end interoperability tests by downloading and processing IFTA, IRP, and Vehicle Inspection transactions with flags set to indicate vehicles should be inspected at the roadside.

Test cases for transaction T0025, T0028 and T0030 will be prepared using dummy DOT numbers. In order not to interfere with the SAFER Certification FTP Server structure, a separate directory has been created on the SAFER Certification FTP server, named “PhaseIIITest”, where the output transaction subdirectories T0025, T0028 and T0030 are created. Test cases will be placed in the corresponding output subdirectories for users to download and use for this test.

5.3.3.1 Configure CVIEW for End-to-End test

The state will configure the CVIEW system to point to the subdirectories under the “PhaseIIITest” directory.

5.3.3.2 Download, Process and Update

The CVIEW system will download the test cases residing in the subdirectories, process them and update the state’s local database.

5.3.3.3 Perform Query at State Office

The state will query the local database to verify that the output files are successfully processed. The state should report the results to the Volpe Center who will enter the information pertaining to the specific test into the State Certification Matrix as required

5.3.3.4 Perform Query at Roadside

The state or the roadside operator will use Aspen, PIQ or the query window to send a request to CVIEW to obtain specific carrier information. A list of the “dummy” DOT numbers will be provided to the states after the states notify Volpe that they intend to perform this optional test.

The state or roadside operator will receive data from the CVIEW system about a specific carrier on the “dummy” list. In real-world situations, this information would be used by the roadside operator to decide if the carrier should be inspected.

5.3.4 Request Certification from FMCSA

Upon completion of the three phases of testing, the Volpe Center will report to the FMCSA, Office of Information Systems (MC-MIS) and request the CVIEW Certification be granted to the state for the processing of SAFER XML output transactions and those specific XML input transactions for which the CVIEW system successfully tested. A copy of the report will be provided to the state and the FMCSA Office of Technology (MC-RTT).

6 State Certification Matrix

The State Certification Matrix below shall be completed by the Volpe Center and submitted to FMCSA (MC-RIS) as part of the request for certification of the state's CVIEW system.

SAFER Interface State Certification Matrix

State: _____

State POC Name: _____

State POC Phone: () _____

Category	Event being tested	Test Phase	Test Case ID	Test Case Name	Expected Results	Actual Results	Status (P / F)
FTP Server							
FTP directory access	Every CVIEW state user will try to login onto the "FTP Directory" to ensure the connectivity is established and the account is working. URL example: ftp://CVIEWxx:****@ftpcert.safers.org/safer Refer to Figure4-1. FTP directory structure in SAFER 4.2 ICD	Phase I			Connectivity should be established. Once connection established, user will be able to access the following directories: SAFER, LOGS, T0019 through T0032		
Transaction Data							
T0019	Input transaction containing IFTA account, name, and address information.	Phase I	XTS19.1	CVIEWxx0000000001.ZIP	SAFER database will be updated successfully		
		Phase II	XTS19.2	TBD (State will provide file name)	SAFER database will be updated successfully		

Category	Event being tested	Test Phase	Test Case ID	Test Case Name	Expected Results	Actual Results	Status (P / F)
T0025	Output transaction containing IFTA account, name, and address information	Phase I	XTS25.1	T0025_20030501100801_1.UD.ZIP	The output transaction file will be found in this directory. Upon successful download and processing, CVIEW local database will be updated		
		Phase II	XTS25.2	TBD (State will provide file name)	The output transaction file will be found in this directory. Upon successful download and processing, CVIEW local database will be updated		
		Phase III	XTS25.3	T0025_20030725102157.UD.XML	The output transaction file will be found in this directory. Upon successful download and processing, CVIEW local database will be updated		
T0020	Input transaction containing IRP account, name, and address information	Phase I	XTS20.1	CVIEWxx0000000002.ZIP	SAFER database will be updated successfully		
		Phase II	XTS20.2	TBD (State will provide file name)	SAFER database will be updated successfully		
T0026	Output transaction containing IRP account, name, and address information	Phase I	XTS26.1	T0026_20030501101001_1.UD.ZIP	The output transaction file will be found in this directory. Upon successful download and processing, CVIEW local database will be updated		

Category	Event being tested	Test Phase	Test Case ID	Test Case Name	Expected Results	Actual Results	Status (P / F)
		Phase II	XTS26.2	TBD (State will provide file name)	The output transaction file will be found in this directory. Upon successful download and processing, CVIEW local database will be updated		
T0021	Input transaction containing IRP fleet account, name, and address information	Phase I	XTS21.1	CVIEWxx0000000003.ZIP	SAFER database will be updated successfully		
		Phase II	XTS21.2	TBD (State will provide file name)	SAFER database will be updated successfully		
T0027	Output transaction containing IRP fleet account, name, and address information	Phase I	XTS27.1	T0027_20030501101201_1.UD.ZIP	The output transaction file will be found in this directory. Upon successful download and processing, CVIEW local database will be updated		
		Phase II	XTS27.2	TBD (State will provide file name)	The output transaction file will be found in this directory. Upon successful download and processing, CVIEW local database will be updated		
T0022	Input transaction containing IRP VIN, registration, proration information	Phase I	XTS22.1	CVIEWxx0000000004.ZIP	SAFER database will be updated successfully		
		Phase II	XTS22.2	TBD (State will provide file name)	SAFER database will be updated successfully		

Category	Event being tested	Test Phase	Test Case ID	Test Case Name	Expected Results	Actual Results	Status (P / F)
T0028	Output transaction containing IRP VIN, registration, proration information	Phase I	XTS28.1	T0028_20030501101401_1.UD.ZIP	The output transaction file will be found in this directory. Upon successful download and processing, CVIEW local database will be updated		
		Phase II	XTS28.2	TBD (State will provide file name)	The output transaction file will be found in this directory. Upon successful download and processing, CVIEW local database will be updated		
		Phase III	XTS28.3	TBD	The output transaction file will be found in this directory. Upon successful download and processing, CVIEW local database will be updated		
T0023	Input transaction containing Carrier e-screen authorization information	Phase I	XTS23.1	CVIEWxx0000000005.ZIP	SAFER database will be updated successfully		
		Phase II	XTS23.2	TBD (State will provide file name)	SAFER database will be updated successfully		
T0024	Input transaction containing Transponder information	Phase I	XTS24.1	CVIEWxx0000000006.ZIP	SAFER database will be updated successfully		
		Phase II	XTS24.2	TBD (State will provide file name)	SAFER database will be updated successfully		

Category	Event being tested	Test Phase	Test Case ID	Test Case Name	Expected Results	Actual Results	Status (P / F)
T0029	Output transaction containing Transponder information	Phase I	XTS29.1	T0029_20030501101601_1.UD.ZIP	The output transaction files will be found in each state's own subdirectory under T0029. States only have the permission to access to their specific directory. Example: CVIEWWA. Upon successful download and processing, CVIEW local database will be updated		
		Phase II	XTS29.2	TBD (State will provide file name)	The output transaction files will be found in each state's own subdirectory under T0029. States only have the permission to access to their specific directory. Example: CVIEWWA. Upon successful download and processing, CVIEW local database will be updated		
T0030	Output transaction containing vehicle IR summary, recent IR and Recent OOS	Phase I	XTS30.1	T0030_20030501080001_1.UD.ZIP	One or more output files will be generated into this directory. Upon successful download and processing, CVIEW local database will be updated		
		Phase II	XTS30.2	TBD	One or more output files will be generated into this directory. Upon successful download and processing, CVIEW local database will be updated		

Category	Event being tested	Test Phase	Test Case ID	Test Case Name	Expected Results	Actual Results	Status (P / F)
		Phase III	XTS30.3	TBD	One or more output files will be generated into this directory. Upon successful download and processing, CVIEW local database will be updated		
T0031	Output transaction containing carrier, cargo, hazmat and review information	Phase I	XTS31.1	T0031_20030501090001_1.UD.ZIP T0031_20030501090001_2.UD.ZIP	One or more output files will be generated into this directory. Upon successful download and processing, CVIEW local database will be updated		
		Phase II	XTS32.2	TBD	One or more output files will be generated into this directory. Upon successful download and processing, CVIEW local database will be updated		
T0032	Output transaction containing licensing and insurance information	Phase I	XTS32.1	T0032_20030501120001_1.UD.ZIP T0032_20030501120001_2.UD.ZIP	One or more output files will be generated into this directory. Upon successful download and processing, CVIEW local database will be updated		
		Phase II	XTS32.2	TBD	One or more output files will be generated into this directory. Upon successful download and processing, CVIEW local database will be updated		