1 Capability

The **Driver Snapshots** capability is:

Establish, maintain, and provide controlled access to driver snapshots that include all or some of these elements:

- Identifiers – Commercial Driver's License (CDL) ID, jurisdiction, biometric data, name, address, date of birth, AKAs (also known as)
- Record access control – who should be able to access; who has accessed the driver record
- Conviction data – information about driving convictions for a driver; include carrier ID
- Crash data – details from specific crash reports; include carrier ID
- Driver license data – data from the driver's license and current status (class, restrictions, exemptions, endorsements, status)
- Driver history – historical information about the person, license, permits, withdrawals, crashes, and convictions
- Inspection data – details from specific inspections; include carrier ID
- Summary safety data – latest summary information from crash, inspection; safety rating; security rating

Use and maintain driver snapshots in all processes (e.g., enforcement, credentialing, hiring, inspection) that require information about drivers.

2 Working Group Recommendations

The Driver Information Sharing Working Group offers these summary recommendations related to this capability:

- Sharing driver data is important to improve safety and security. However, privacy concerns must be addressed. Acceptable intended use of the data must be specified and penalties for misuse defined. The data must be protected. Drivers and other stakeholders must be included in the discussions. The process of defining and designing an approach to improve the sharing of driver information must be open and transparent.
- Development of a "driver safety rating" is critical to improving safety, security, and productivity.
- Before embarking on any particular driver information sharing approach, stakeholders should agree on specific data elements, definitions, syntax, format constraints, and semantics that explain the intended business use of the data elements for each destination

system and user type. The working group could tackle this effort as part of follow-on efforts to this report.

- The "Snapshot Light" solution option is recommended for supporting the Driver Snapshots capability. It builds on Core Commercial Vehicle Information Systems and Networks (CVISN) capabilities and interfaces and would provide quick information about a driver for roadside screening.
- The group also discussed briefly the notion of a hybrid solution incorporating elements of the Snapshot Light solution for this capability and the "Provide facilitated centralized query" option recommended in the Access to Driver Data capability report (see reference 1). Those who request driver data via Query Central could be provided not only the current driver license data from the state of record but also the limited driver snapshot proposed in the Snapshot Light solution.
- Two activities related to this capability are proposed for near-term funding:
  - Driver Safety Rating Focus Group
  - Snapshot Light Prototype
- The working group supports both the Snapshot Light and Facilitated Centralized Query options for sharing driver information and recommends that Federal Motor Carrier Safety Administration (FMCSA) explore hybrids of the two solutions in prototype activities.

3 Concept of Operations

Note: This section is identical to the comparable one for the **Access to Driver Data** capability.

The term concept of operations (ConOps) means operational attributes of the system from the operators' and users' views. The ConOps allows for the use of a variety of technologies. There may be potential benefits to be gained by using some sophisticated technologies, but only if the technologies are part of a well-conceived and vetted set of practices, are thoroughly understood and tested, and are implemented and used correctly. This section summarizes the proposed concept of operations.

Existing systems contain much of the information needed to achieve the goals of the Expanded CVISN initiative. To increase information sharing, expand, merge, establish interfaces between, or enhance existing **information management systems** [e.g., Motor Carrier Management Information System (MCMIS), Commercial Driver's License Information System (CDLIS), Safety and Fitness Electronic Records (SAFER), Commercial Vehicle Information Exchange Window (CVIEW), Performance and Registration Information Systems Management (PRISM), International Registration Plan (IRP) and International Fuel Tax Agreement (IFTA) clearinghouses] to include:

- Role-based access to services using single sign-on
- Open standards for information sharing

- Improved and flexible user interfaces (e.g., provide default look and feel based on user's role; allow user to tailor)
- Standardization around a small number of standards. This gives each state the flexibility to work within its overall statewide architecture, but still encourages commonality among states' systems and approaches.
- Collection of data once and frequent reuse (e.g., collect census data from a carrier and re-use that data from a single source whenever it's needed)
- Consistent level of service regardless of time-of-day or day-of-year
- Improved access to data about all commercial drivers
- Consistent identification of carrier, driver, vehicle, and cargo
- Association of entities that are related during a trip (e.g., John Driver working for Carrier XYZ driving vehicle with plate 1234567 registered in Maryland hauling trailer with plate 8901234 registered in Delaware)
- Access to up-to-date credentialing information (e.g., permits).

To improve the quality of information and to improve access, develop, expand, merge, or enhance **data collection and reporting systems** used in the field [e.g., ASPEN, Carrier Automated Performance Review Information (CAPRI)] to include:

- Open standards for authorized data collection and reporting
- Access to driver snapshots by authorized users for approved purposes
- Out-of-service (OOS) processing
- Uniform citation reporting
- Uniform crash reporting
- Hours of service compliance evaluation
- Interface with electronic on-board systems
- Wireless technology.

Look for successes within innovative programs and build on or adapt their business models for broader use. Categories of programs/systems to review include:

- Electronic toll collection systems (e.g., E-ZPass)
- Electronic credentialing systems for multiple credentials [e.g., One-Stop Credentialing and Registration (OSCAR)]
- Regional data-sharing systems [e.g., extensible CVIEW (xCVIEW)]
- Roadside information reporting systems (e.g., ASPEN)

- Port scheduling/access programs (e.g., PierPass)
- Freight security improvement programs [e.g., Operation Safe Commerce (OSC)]
- Cross-program technical interchange (e.g., CVISN/PRISM)
- Border-crossing improvement programs [e.g., Free and Secure Trade (FAST)]
- Data challenge and correction (e.g., DataQs).

Review and build on technology lessons learned. Categories of programs/initiatives to review include:

- Recent operational tests [e.g., FMCSA's Hazardous Materials (HazMat) Op Test]
- Intelligent Transportation Systems (ITS) initiatives [e.g., Vehicle Infrastructure Integration (VII)]
- Applications and uses of standards [e.g., Dedicated Short-Range Communications (DSRC) standards]
- Technology transfer opportunities [e.g., Federal Rail Administration's (FRA's) railroad track status reporting]
- Commercial Vehicle Operations (CVO) infrastructure deployments (e.g., e-screening)
- Broader transportation infrastructure deployments (e.g., e-toll collection)
- Data sharing models (e.g., CDLIS).

Employers may choose to use nongovernmental information to help in the evaluation of prospective drivers (e.g., personality assessments, references).

4 Requirements

Note: This section is identical to the comparable one for the **Access to Driver Data** capability.

Discussions with the members of the Driver Information Sharing Working Group established by FMCSA via the ITS/CVO 2005 Deployment Showcase established the requirements stated in this section. During the initial discussion, we did not separate the requirements between the Driver Snapshots and Access to Driver Data capabilities. In follow-on discussions the group decided that the basic requirements for the two capabilities are the same.

Various business processes need information about a driver.

- Carriers need driver information for pre-employment and periodic qualification checks. In addition, carriers need information whenever certain events occur (e.g., conviction, withdrawal, OOS order) for their drivers.

- Government agencies require driver information during driver licensing processes, compliance reviews, medical qualification waiver evaluation, enforcement activities (e.g., traffic stops), legal activities (e.g., preparation for a case, adjudication) and inspections.
- Roadside enforcement would like to know in advance what driver is behind the wheel (a real-time identification issue that is not in scope for this capability) and consider driver safety risk when selecting vehicles for inspection. Electronic screening algorithms should be updated to consider driver safety risk. Roadside activities require up-to-date information for enforcement action.
- Insurance companies need information about drivers to more accurately match cost and risk.
- Leasing companies need information about drivers to evaluate potential leasing arrangements with those drivers.

Today there are some data quality problems regarding driver data. Implementation of either driver information sharing capability should address the data quality problems if possible.

- Carriers are required to review a prospective driver's history as part of the hiring process and annually review every driver's record. Some states' responses to carriers' requests for driver data are not timely, so carriers sometimes use service bureaus like United States Investigations Service (USIS)/DAC, USSEARCH, ChoicePoint, or Employment Screening Resources to accomplish the driver record checks. The service bureaus' reports do not always match state-held records. Additionally, the service bureau records lack important data. They do not contain information about motor carrier enforcement such as inspection and OOS information. Some states do not maintain crash information, so crash information on service bureau records is spotty. Further, service bureau records are dated. Typically, service bureaus purchase records annually.
- Roadside data (e.g., speeding, OOS order, other inspection results) associated with a previous carrier do not follow the driver. There is no readily accessible, user-friendly source for driver inspection information.

There are many potential driver data elements that could be shared. The working group reviewed the list and decided that these represent the main categories:

- *Identifiers* – CDL ID, jurisdiction, biometric data, name, address, date of birth, AKAs
- *Driver history* – historical information about the person, license, permits, withdrawals, crashes, convictions
  - Include crashes from past 5 years; date, severity, location for each crash; need to be able to access full crash report; include carrier ID, crash circumstances, information collected about the driver when involved in a crash
  - Include driving convictions from past 5 years, carrier ID
- *Driver license data* – data from the driver's license and current status (class, restrictions, exemptions, endorsements, status)

- *Inspection data* – details from specific inspections; include carrier ID
- *Summary safety data* – latest summary of information from crash and inspection reports; safety rating (proposed new item); security rating (potential new item)
  - # of crashes in past 5 years
  - # of inspections in past 3 years
  - # of driver OOS in past 3 years
  - # of selected vehicle OOS in past 3 years (selection based on which conditions could have been observed by the driver)
- *Access control* – who should be able to access and who has accessed the driver's record.

The working group suggests that sharing limited medical waiver data (name, date of birth, unique identifier, waiver status, waiver expiration, waiver processing date) be considered as a potential requirement. Sharing such information must be in accordance with existing federal and state regulations.

Other requirements for driver data sharing:

- Sharing of driver data must comply with the federally codified Drivers Privacy Protection Act (http://uscode.house.gov/download/pls/18C123.txt) and related state laws.
- Data access should be limited based on a user's role and authority.
- Only authorized users should be able to access information to perform their duties.
- Use of data for other than authorized purposes should be subject to penalties.
- Data integrity must be maintained and processes for challenging errors must be readily available.
- Data must be protected from inadvertent disclosure.
- Driver should be able to specify which industry users may access the information.
- Driver should be able to see his/her own data and challenge information that they believe is incorrect or inaccurate. Notes about the challenge should be included in the record.
- Driver should be able to see a report showing who has accessed the information.
- It should not be assumed that every driver has Internet access. Other methods of access and defining who from industry may access their records should be provided.
- If a carrier rejects a driver's application due to driving record data, the carrier should provide the driver a copy of the report accessed.
- Always link the driver to the carrier when collecting roadside information about the driver.
- Data shared about drivers should be the same whether the driver operates intrastate, interstate, or internationally.

- According to preliminary results from the FMCSA-sponsored Driver Violation Notification/Employer Notification Service project, carriers were interested in:
  - Exception-based information or information provided on change.
  - Seeing a full report when an adverse event occurs (e.g., conviction), so that the event can be viewed in context. Even if the event occurred when the driver was on a trip for a different carrier, all carriers for whom the driver currently works would want to see the data.
  - Carriers would like to have access to violation data (moving and safety violations). However, the information is not normally actionable until a conviction is reached.

5 Potential Solution Alternatives

Several potential solution options for the **Driver Snapshots** capability were identified. The working group decided that these are worth further investigation:

- Option 1: Replicate driver data in a central snapshot repository (e.g., SAFER, MCMIS) (AKA Full Snapshot)
- Recommended Option 2: Replicate a limited set of driver data in a central snapshot repository (e.g., SAFER, MCMIS) (AKA Snapshot Light).

For each potential solution option, the architecture and possible impacts on federal, state, and industry systems/business processes are summarized. When asked to choose between Options 1 and 2, the group selected Option 2, Snapshot Light.

It should be noted that the working group supports the “Provide facilitated centralized query” option now described in the **Access to Driver Data** capability report as an excellent alternative for driver information sharing as well. The group also discussed briefly the notion of a hybrid involving elements of the Snapshot Light solution and the facilitated centralized query option recommended for the Access to Driver Data capability. Those who request driver data via Query Central could be provided not only the current driver license data from the state of record but also the limited driver snapshot proposed in the Snapshot Light solution.

The working group decided that the following options are not worth pursuing:

- Establish access to individual systems of record that hold driver data
- Replicate driver data in regional or state snapshot repositories (e.g., CVIEW).

For the options that the group does not recommend, the descriptions and reasons for rejecting the options are included below, but no further analysis will be provided in subsequent sections.

5.1 Option 1: Replicate driver data in a central snapshot repository (AKA Full Snapshot)

In this option, a centralized information management system (SAFER or MCMIS) would store, or collect upon legitimate request, the full driver snapshot data set. If SAFER stores driver snapshots, all the data would be replicated there since SAFER is not the authoritative source for any information. If MCMIS stores driver snapshots, it is already the authoritative source for inspection data, but would replicate other driver snapshot information. Data for which states are the authoritative source would be pushed to the central repository upon change, or would be supplied when requested by the repository system. The central repository system would merge data from multiple sources into a snapshot. Automated processes would be required to reconcile data from different sources and match records properly. Manual intervention might also be required. The central repository would store the full driver snapshot. The central repository would offer subscription services so that users could subscribe to receive snapshot updates upon change. The central repository would offer query services so that users could request a specific snapshot and have that query managed in near real-time either by retrieving an existing snapshot from the repository or by the repository gathering fresh data from the authoritative sources. When the central repository handles a query or fulfills a subscription for driver data, it would inform the state of record ("access info" on the diagram) so that the driver could be notified. Subscription and query services would be provided based on user role and authentication. The central repository would store snapshots for all CDL holders. Drivers could control what private entities/people are able to access their records and see who has accessed their records. A common algorithm would be provided to determine driver safety scores. Figure 5-1 illustrates the high-level architecture for this option.

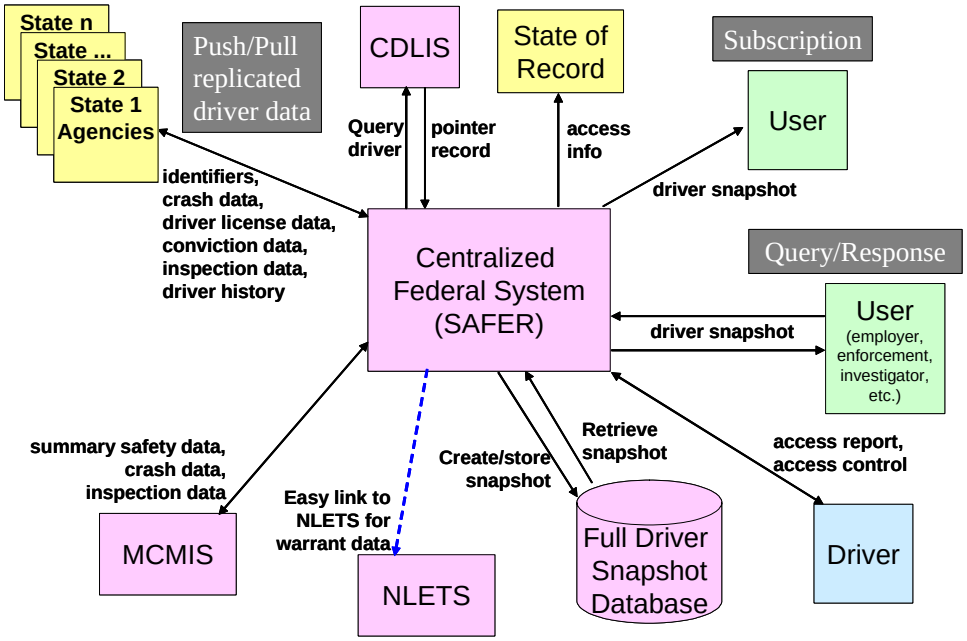

Figure 5-1. Option 1: Full Snapshot

Under this option, the impact on federal systems would be significant, since no driver snapshot structure exists and since very few driver data elements are currently stored in federal systems. SAFER (assumed to be the central repository) would manage the full driver snapshot information for all drivers with CDLs. MCMIS or its equivalent would push summary safety data to SAFER upon change and would also compute updated driver safety ratings for drivers about whom it has sufficient data. Safety ratings would be updated periodically. State systems would be changed to push driver data updates to fulfill the full snapshot to the central repository and to respond to queries from the central repository. The central repository would manage access to information according to business rules. Systems that support compliance reviews and medical waiver processing would be modified to use driver snapshots. State systems would also be changed to use the central repository to support roadside operations and for other driver information checks. Industry systems would be changed to access the single central repository.

Under this option, states could use their CVIEW or equivalent to manage the interface with SAFER on behalf of other systems in the state. States could choose to replicate driver snapshots in their own systems in addition to keeping SAFER up to date.

5.2 Recommended Option 2: Replicate a limited set of driver data in a central snapshot repository (e.g., SAFER) (AKA Snapshot Light)

In this option, a centralized information management system (e.g., SAFER) would store or collect upon legitimate request limited driver snapshots. The data would be replicated since SAFER is not the authoritative source for any information. This option differs from Option 1 in the quantity of information replicated in the central repository. The limited driver snapshot would include the data needed by the roadside for screening.

- Driver name
- Date of birth
- License ID
- License jurisdiction
- License status
- # of crashes in past 5 years (FMCSA provides if interstate)
- # of inspections in past 3 years (FMCSA provides if interstate)
- # of driver OOS in past 3 years (FMCSA provides if interstate)
- # of selected vehicle OOS in past 3 years (selection based on which conditions could have been observed by the driver; FMCSA provides if interstate)
- safety rating for driver (proposed new item FMCSA would provide if interstate).

Data for which states are the authoritative source would be pushed to the central repository upon change, or would be supplied when requested by the repository system. The central repository

system would merge data from multiple sources into a limited snapshot. The central repository would store the limited driver snapshot. The central repository would offer subscription services so that users could subscribe to receive the limited snapshot updates upon change. The central repository would offer query services so that users could request a specific snapshot and have that query managed in near real-time by retrieving an existing snapshot from the repository. The user could request a full snapshot that contains all the data identified in Option 1. To fulfill that request, SAFER would query the authoritative state and/or federal source systems and merge the results into a snapshot format. Automated processes would be required to reconcile data from different sources and match records properly. Manual intervention might also be required. SAFER would interface with CDLIS to request data from state driver licensing systems. When the central repository handles a query or fulfills a subscription for driver data, it would inform the state of record ("access info" on the diagram) so that the driver could be notified. Subscription and query services would be provided based on user role and authentication. The central repository would store the limited snapshots for all CDL holders. Drivers could control what private entities/people are able to access their records and see who has accessed their records. A common algorithm would be provided to determine driver safety scores. Figure 5-2 illustrates the high-level architecture for this option.

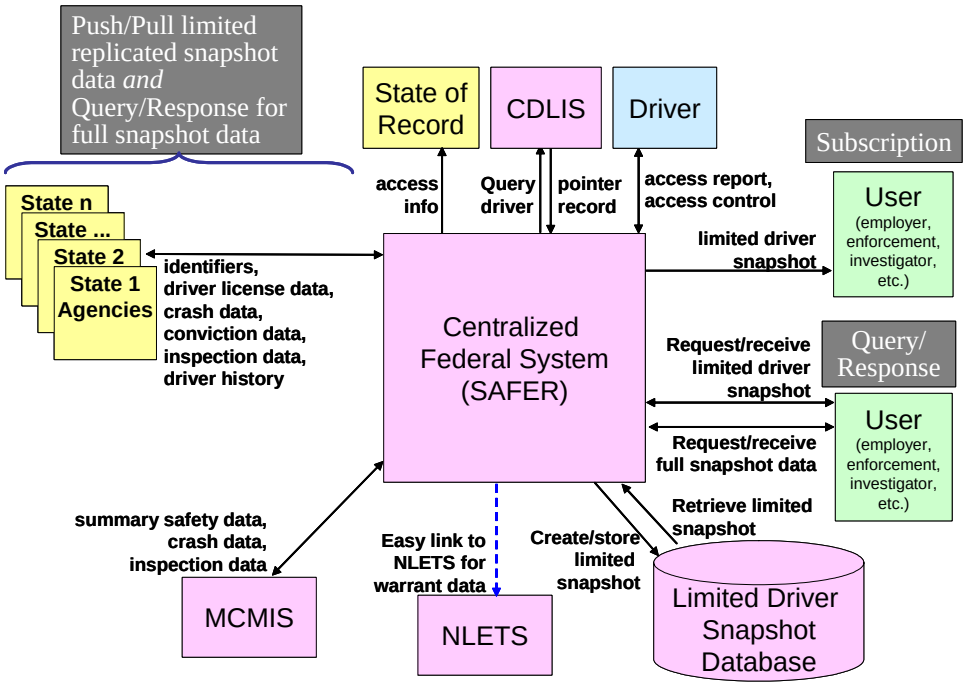

Figure 5-2. Recommended Option 2: Snapshot Light

Under this option, the impact on federal systems would be significant, since no driver snapshot structure exists and since very few driver data elements are currently stored in federal systems. The impact should be somewhat less than under Option 1, since less data is stored in the limited snapshot. However, SAFER (assumed to be the central repository) would still connect to all the state and federal systems shown in Option 1 to manage snapshots for all drivers with CDLs. The

central repository would manage the limited driver snapshot storage, manage the query/response process for full snapshot information, and package the responses into a standard snapshot structure for delivery to the requester. MCMIS or its equivalent would push summary safety data to SAFER upon change sufficient to fill the MCMIS fields in the limited snapshot. As in Option 1, MCMIS would also compute updated driver safety ratings for drivers about whom it has sufficient data. Safety ratings would be updated periodically. State systems would be changed to push driver data updates to fulfill the limited snapshot to the central repository and to respond to queries from the central repository. The central repository would manage access to information according to business rules. Systems that support compliance reviews and medical waiver processing would be modified to use driver snapshots. State systems would be changed to push limited driver data updates to the central repository and to respond to queries from the central repository. State systems would also be changed to use the central repository to support roadside operations and for other driver information checks. Industry systems would be changed to access the single central repository.

Under this option, states could use their CVIEW or equivalent to manage the interface with SAFER on behalf of other systems in the state. States could choose to replicate the limited driver snapshots in their own systems in addition to keeping the data in SAFER up to date.

5.3 Moved to Access to Driver Data: Provide facilitated centralized query

In this option, a centralized query service would be provided for all authorized users. Query Central is a model. No driver snapshots would actually be stored by the query service. Thus, this option was moved to the other capability report: **Access to Driver Data**.

5.4 Rejected Option: Establish access to individual systems of record that hold driver data

Different state systems store data related to drivers. Systems include those that manage driver license information, collect and manage crash data, collect and manage citation and conviction information, and SAFETYNET. In this option, these systems would be modified to allow access for all legitimate users of driver information. The user or system that wants “snapshot” data would retrieve and integrate the data. Only the user or system that wants the snapshot might store the snapshot for later use.

Under this option, the impact on federal systems would be minimal, since driver inspection data are assumed to be provided from SAFETYNET instead of SAFER or MCMIS. A common algorithm would be provided to determine a driver safety score. Many state systems would be changed to enhance access to driver information, provide standard data outputs, and monitor and control access based on a user’s role and authority. State systems might also be changed to

access other states' systems for driver licensing checks and to retrieve driver data for roadside operations. Industry systems would be changed to access the different systems in each state.

This option was rejected because of its widespread impact and complexity. The solution would require information seekers to access multiple systems in many jurisdictions. It would require significant changes to systems in every state. It is unlikely that all agencies in all states would achieve the same level of success in opening their systems to external access. The solution would be too costly to consider further.

5.5 Rejected Option: Store driver data in regional or state snapshot repositories

For this option, each state or regional CVIEW or similar repository system would store, or collect upon legitimate request, the data identified for driver snapshots. Since such systems are not authoritative sources, all the driver snapshot data would be replicated in the state or regional snapshot repository. Data would be pushed to the repository by the appropriate authoritative source system, or would be supplied when requested by the repository system. The repository would merge data from multiple sources into a snapshot. The repository would offer subscription services so that users could subscribe to receive snapshot updates upon change. The repository would offer query services so that users could request a specific snapshot and have that query managed in near real-time either by retrieving an existing snapshot from the repository or by the repository gathering fresh data from the authoritative sources. Subscription and query services would be provided based on user role and authentication. The repository would hold snapshots for all commercial drivers licensed in the jurisdiction(s) associated with the state or regional repository. Each state or regional repository would handle queries from other repositories.

Under this option, the federal MCMIS or SAFER system would be changed to supply snapshot information from inspections to the state or regional repositories. A common algorithm would be provided to determine driver safety scores. Each state or regional repository would manage driver snapshot information including inspection data, census data, license status, driver history, crash data, citation data, and violation data associated with all commercial drivers licensed in the jurisdiction(s) associated with that state or regional repository. The state or regional repository would manage access to information according to business rules. Systems that support compliance reviews and medical waiver processing would be modified to use driver snapshots from the appropriate state or regional repository. State systems would be changed to push driver data updates to the state or regional repository and to respond to queries from the state or regional repository. State systems would also be changed to use their repository for driver licensing checks and to support roadside operations. Industry systems would be changed to access the state or regional repositories where drivers of interest are licensed. Each state or regional repository would handle queries from other repositories.

This option was rejected because it is not consistent with the CVISN architecture and because of the risk that different states/regions would develop different snapshots and access methods.

Unless all states/regions work together to formulate and implement standards for information sharing, a national solution may never be achieved. The group believes that Option 1 and Option 2, which build on the existing SAFER approach, have stronger technical and institutional merit.

6 Cost-Benefit Analysis

The following table provides a high-level cost-benefit analysis for each acceptable solution option identified in the previous section. Putting the issues described in Section 8 aside, the common pros and cons across all options include:

- Pro: Improve the safety and security of commercial vehicle operations by providing driver snapshot information to authorized users or system
- Con: Incur significant costs to define, implement, and achieve standards for driver information sharing
- Con: Privacy regulations and concerns may be difficult to address

The cost figures are rough estimates provided by working group members.

- Low means less than $100K
- High means more than $1M
- Medium is everything in between.

Option	Pro	Con	Cost
1 (Full Snapshot)	All: Leverages existing CVISN architecture and concepts. Federal: Builds on existing SAFER system. Opportunity to integrate with and leverage Creating Opportunities, Methods, and Processes to Secure Safety (COMPASS) initiative. State: Builds on existing CVISN interfaces. Industry: Single interface with central repository.	All: Significant replicated data; very difficult to keep current. Using inaccurate information could bring forth law suits. Federal: Significant changes to an existing system. Significant data storage and information management. State: Must push data from several state systems to federal repository and respond to queries. Industry: ---	Federal: Development costs – High. Maintenance costs – Medium. State: Development costs – Medium. Maintenance costs – Medium. Industry: Low

Option	Pro	Con	Cost
2 (Snapshot Light)	All: Leverages existing CVISN architecture and concepts. Less replicated data than Option 1. Federal: Builds on existing SAFER system. Opportunity to integrate with and leverage COMPASS initiative. State: Builds on existing CVISN interfaces. Less driver data to push to SAFER than Option 1. Industry: Single interface with central repository.	All: Some replicated data; still difficult to keep current. Using inaccurate information could bring forth law suits. Federal: Significant changes to an existing system. Significant information management. State: Must push limited data from several state systems to federal repository and to respond to queries. Industry: ---	Federal: Development costs – Medium. Maintenance costs – Low. State: Development costs – Medium. Maintenance costs – Low. Industry: Low

7 Business Case

Drivers are critical to assuring safe and secure commercial vehicle operations, but concerns about data privacy initially limited the use of data to focus on high-risk drivers. Carriers are required to assess drivers prior to hiring, but have insufficient information. Aside from the obvious, the more information a carrier has in making a decision of hire/no hire and qualified/not qualified, the better. Carriers will come to rely on the accuracy of information they receive from reliable sources. The more and accurate information (good or bad) a carrier has when making these decisions, the better they can serve the public not only with reliable service but **safe** reliable service. Carriers would like access to violation data so that they can take action (e.g., counseling, training) with the driver involved; however, some violation data is held within the court system. The key is to share only factual information with carriers and let them make the final decision. If this information can be transmitted through a single reliable data source, it could be transmitted with a minimum of delay thereby making a decision sooner, which is only fair to the applicant.

Commercial driver licensing processes are only beginning to address security concerns. Information about drivers is scattered across many information systems, making it difficult to assess in a real-time setting. Information about commercial drivers is routinely collected only in association with licensing and safety inspections. It is doubtful that the snapshot concept will support all the information requirements associated with driver licensing.

Getting withdrawn drivers off the road will have tremendous, measurable benefits in highway safety. It would also provide a revenue stream. Getting wants and warrants out to the roadside also could provide substantial public safety benefits. There is a national security argument to be made for providing immediate access to determine if the individual being stopped is on a terrorist watch list. How can prosecutors assert a charge based on history if the history is not

available? Similarly, how can judges base sanctioning decisions on history if the history is not available?

The situation is ripe for change, and the user community is clamoring for better driver information sharing. Any solution options for full driver snapshots involve significant investment overall. Limiting the data in a driver snapshot to the highest priority data elements should reduce costs. Once the initial investments have been made to upgrade the systems that collect, store, and use driver snapshot information, recurring costs to sustain and maintain those systems are likely to correlate with the number of data elements to be shared and the number of systems involved in snapshot creation, maintenance, and use. The complexity of the design and ease of use will also affect recurring costs. Attention should be paid to devising simple and stable interfaces.

8 Issues

8.1 Institutional Issues

Many different agencies and systems manage driver data, which makes the task of creating, managing, and sharing driver snapshots extremely complex.

Laws about access to personal information vary by state. It is imperative that driver data be used only for legitimate (and clearly defined) purposes. Once driver data sharing is improved, it may be difficult to control how the data are used. Those who abuse the access to driver data or misuse the information should be subject to penalties and restrictions. Sharing medical waiver data would pose additional challenges since such information is subject to federal and state laws. Protection of drivers' rights and mechanisms for drivers to waive their rights should be considered in designing the processes and systems for sharing driver data. Issues about who is authorized to update, change, and query data must be addressed. Control of data stored locally (as opposed to in a central repository) must be considered. Revenue to the states must not be lost, or states will not support any new approach.

States agreed to a minimum common set of data elements about crashes, but there are some crash data elements that are unique to a state.

Information collected about citations and convictions varies, to some extent, by state. Many states do not have centralized systems for tracking citations with moving violations. In some cases, each police organization has its own citation tracking system, which may or may not be automated. After a citation is issued to a driver, the court system may reduce the offense to a lesser charge. There is no nationwide, uniform, reliable method to match citations with eventual convictions.

Ongoing training for enforcement and judicial system personnel is required to keep up with changes in the commercial motor vehicle code and the impacts of changing a citation to a lower-level infraction.

Background checks are required for drivers of hazardous materials cargo, but are not required for all commercial drivers.

Medical examinations are sometimes performed by doctors unfamiliar with regulations regarding commercial driver qualifications.

Rulemaking will probably be required to implement a driver safety rating. Outreach will be required to discuss the algorithm used to compute the safety rating. Potential users of the rating must understand how the rating is intended to be used, what factors influence the rating, and latency issues.

The solutions defined in this report are focused on CDL holders, not on those who may drive a commercial motor vehicle without a CDL.

There are national systems (CDLIS, Problem Driver Pointer System) that provide both tremendous opportunities for a low-cost driver snapshot implementation and a whole set of institutional barriers. American Association of Motor Vehicle Administrators (AAMVA) is considering a redesign of CDLIS and an All-Drivers System; efforts should be coordinated.

8.2 Technical Issues

There is no existing structure for driver snapshots. Most of the states' authoritative source systems that manage the data to be provided in a driver snapshot do not currently support outside access from different kinds of users or other information systems. There are no common database structures or open interface standards for crash, citation, and conviction data, which may make it difficult to extract information about a particular driver from some reports. The data quality problems described in Section 4 exist across the nation in many systems. Not all data about all CDL holders are held in either the state or federal systems. For instance, only federally-reportable crash data are held in MCMIS. To determine a safety rating, information may have to be merged from a mix of state and federal systems. The algorithm to compute a driver safety rating should be run by a centralized system that merges information, but that system may not have sufficient information to compute the rating for all drivers. There will be an ongoing challenge to reconcile information from different sources, match and merge records, and remove errors from the systems that share information about drivers.

9 Deployment Strategy

In deploying the Driver Snapshots capability, several aspects should be considered:

Improve data quality and integrity:

- Establish a consistent set of data elements that are common across information systems and analysis applications.
- Expand the use of standard identifiers for entities visible at the roadside (carrier, vehicle, driver, cargo, chassis) to link related information.
- Make information collection, access, and use consistent across interstate, foreign, and intrastate operations.
- Capture data electronically as close to the source as possible; once information is available electronically, it should be re-used instead of re-entered manually.
- Expand standard procedures and tools for reviewing, detecting problems in, and correcting errors in publicly-held data.
- Expand the use of on-line tools that provide industry and drivers with the ability to challenge and correct their own census, inspection, crash, and citation information.
- Control access to sensitive information.
- Limit use of data to approved business functions.
- Information security must be incorporated into all parts of the process.

Work together and share lessons learned:

- Work with stakeholders to define and deploy common data elements and interoperable business processes for all areas of CVISN expansion.
- Establish standardized terminology and common requirements for data collection, access, quality checks, and making corrections.
- Coordinate standards-related activities with appropriate standards development organizations.
- Actively solicit lessons learned from “early adopters” of CVISN and expanded CVISN concepts, and determine how to apply those lessons more broadly.
- Actively engage stakeholders in identifying priorities, proposing solutions, and participating in prototype projects.
- Proactively reach out to stakeholders who may be affected by changes to systems or processes that are under discussion.
- Learn from other ITS activities about solutions applicable to CVO.

Deploy targeted solutions incrementally:

- Select information-sharing options based on users’ needs and available technology (e.g., proactive data-provider “data push” versus user-initiated “data query”).
- Prototype proposed solutions and link to existing capabilities.

- Consider small-scale solutions that can be expanded or serve as models for national deployment.
- Build in metrics to assess real improvements.
- Provide access to on-line analysis tools.
- Provide an approach that allows states to improve the quality of data sent to aggregation sources while continuing to maintain interaction with other state systems that may insist upon "lower quality" or "nonstandard" data.

Use appropriate technology to improve operations:

- Equip commercial vehicles with standard DSRC and other technologies, enabling a multitude of safety, security and productivity applications.
- Deploy interoperable technologies to support CVISN and other related CVO activities.
- As products become available, consider 5.9 GHz DSRC as an enabling technology for roadside-to-vehicle, vehicle-to-roadside, and vehicle-to-vehicle data exchange.
- Apply new and emerging wireless capabilities [e.g., Bluetooth, Wireless Fidelity (Wi-Fi), Global Systems for Mobile Communications (GSM)] and on-board technologies to improve on-road and roadside operations and reduce costs.

The working group recommends two activities related to the Driver Snapshots capability. The first activity focuses on determining an approach for a driver safety rating. The second activity involves prototyping the Snapshot Light option.

9.1 Driver Safety Rating Focus Group

Recent research should be examined for possible approaches to determining a driver safety rating. The data and results from several studies should be reviewed by a cross-section of stakeholders including drivers, carriers, shippers, enforcement, policy makers, and researchers. For example, these studies (and others suggested by group members) should be reviewed:

- (Ongoing project) Brenda Lantz, sponsored by American Transportation Research Institute (ATRI), "The Development of a Commercial Vehicle Driver Behavior-Based Indicator to Predict Future Crash Involvement and Identification of Effective Enforcement Actions."
- Brenda Lantz, Jeff Loftus and Tom Keane, *Development and Implementation of a Driver Safety History Indicator into the Roadside Inspection Selection System,* 2004, http://www.ugpti.org/tssc/projects/drivesafe.php.
- Brenda M. Lantz and Michael W. Blevins, *An Analysis of Commercial Vehicle Driver Traffic Conviction Data to Identify High Safety Risk Motor Carriers*, 2001, http://www.ugpti.org/research/carrier/projects/mcp029.php.

- Ronald R. Knipling, Linda N. Boyle, Jeffrey S. Hickman, James S. York, Carmen Daecher, Erik C. B. Olsen, and Tammy D. Prailey, *Commercial Truck And Bus Safety Synthesis Program, Synthesis 4, Individual Differences and the "High-Risk" Commercial Driver*, research sponsored by the Federal Motor Carrier Safety Administration, © Transportation Research Board of the National Academies, ISBN 0-309-08810-0, 2004, http://trb.org/publications/ctbssp/ctbssp_syn_4.pdf.
- Touchstone Consulting Group, Inc., for FMCSA, *Comprehensive Safety Analysis 2010 Listening Sessions – Final Report*, 7 March 2005, http://dms.dot.gov/search/document.cfm?documentid=321212&docketid=18898.

The focus group should review the analysis results and try to devise a tool that would help with driver roadside screening, driver inspection selection, and driver hiring. Brenda Lantz, AAMVA, Volpe, and Colorado expressed interest in participating in this activity.

9.2 Snapshot Light Prototype

A project should be developed to prototype the "Snapshot Light" option for the Driver Snapshots capability. There are several goals for the prototype:

- To identify an initial set of driver data that should and can be shared
- To demonstrate a workable approach to sharing driver data
- To demonstrate the value of sharing driver data
- To address privacy concerns and regulations
- To identify risks and vulnerabilities in accessing, using, storing, and/or sharing driver data.

The prototype should limit the amount of data shared via snapshots but should include multiple systems at the state and federal levels to assess the feasibility of a broader implementation. The prototype should be coordinated with related efforts to specify data elements, definitions, syntax, format constraints, and semantics that explain the intended business use of the data elements for each destination system and user type. Several industry representatives should be involved in the prototype to evaluate the impact on service bureaus, large carriers, and smaller carriers. Snapshots for interstate, intrastate, and foreign drivers should be included in the prototype. Drivers must be fairly represented on the project team. AAMVA has extensive experience in consensus building and information sharing where driver data are concerned and should be part of the project team.

Volpe Center staff working on data quality issues and AAMVA expressed interest in participating in this activity.

10 References

1. JHU/APL, *Expanded CVISN Driver Information Sharing Capability Report: Access to Driver Data,* SSD-PL-05-0195, June 2005.