1 Capability

The **Access to Driver Data** capability is:

Improve enforcement's and carrier's access to driver information to target driver safety risk.

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 "Provide facilitated centralized query" solution option is recommended for supporting the Access to Driver Data capability. It builds on existing Query Central and Commercial Driver's License Information System (CDLIS) capabilities and interfaces and would provide enhanced information about a driver.
- The group also discussed briefly the notion of a hybrid involving the recommended "Provide facilitated centralized query" solution for this capability and the "Snapshot Light" solution recommended for the Driver Snapshots capability (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 (described in the **Driver Snapshots** capability report)
  - Facilitated Centralized Query 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 **Driver Snapshots** 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), 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 non-governmental 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 **Driver Snapshots** 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 Snapshot 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, out-of-service 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* – Commercial Drivers License (CDL) ID, jurisdiction, biometric data, name, address, date of birth, AKAs (also known as)
- *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

The assumption for the **Access to Driver Data** capability is that all driver data will **not** be gathered into a single snapshot. Only potential solution alternatives that are distinctly different from the options described for the Driver Snapshot capability are discussed here. Several potential solution options for the **Access to Driver Data** capability were identified. The working group decided that these are worth further investigation:

- Option 1: Improve access to federally-held driver data
- Option 2: Provide a "full driver report" from federal systems
- Recommended Option 3: Provide facilitated centralized query.

For each potential solution option, the architecture and possible impacts on federal, state, and industry systems/business processes are summarized. When asked to choose among the three options, the group selected Option 3, "Provide facilitated centralized query."

It should be noted that the working group supports the "Snapshot Light" option described in the **Driver Snapshots** capability report (reference 1) as an excellent alternative for driver information sharing as well. The group also discussed briefly the notion of a hybrid involving the recommended "Provide facilitated centralized query" solution and the Snapshot Light solution recommended for the Driver Snapshots 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 this option is not worth pursuing:

- Augment CDLIS or driver licensing systems to access SAFETYNET.

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

5.1 Option 1: Improve access to federally-held driver data

In Option 1, access to driver data held in MCMIS would be improved. Information from MCMIS would be indexed for streamlined retrieval and presentation in reports using open standards. Authorized users would be able to search for driver information stored in inspections and crash reports, regardless of where the driver is licensed or what carrier he/she works for. Query parameters would include the driver's name and/or license ID and (optionally) license jurisdiction. Carrier, state driver credentialing, enforcement, and service bureau personnel and systems would be able to register to be authorized to access the driver data. Drivers could control what private entities/people are able to access their records, and see who has accessed their records. Users who want driver license status and conviction data would access state systems via CDLIS or other existing mechanisms.

For each driver, the information provided from the federal system would include:

- Driver name, license ID, license jurisdiction
- Summary safety data
- Critical data from individual inspections
- Critical data from each federally-reportable crash report.

This new/expanded federal capability would not provide:

- Current CDL status
- Conviction information
- Moving violations that are not related to an inspection
- Immediate access to the details from inspections or crashes. An easy link to existing systems (e.g., SAFER) could be provided so that authorized users could use the existing capabilities to retrieve the details that are already available.

FMCSA would offer query services so that users could request information about a specific driver and have that query managed in near real-time by retrieving record(s) from the authoritative sources. Query services would be provided based on user role and authentication. FMCSA would provide information only for drivers about whom data are held in FMCSA systems. Figure 5-1 illustrates the high-level architecture for this option.

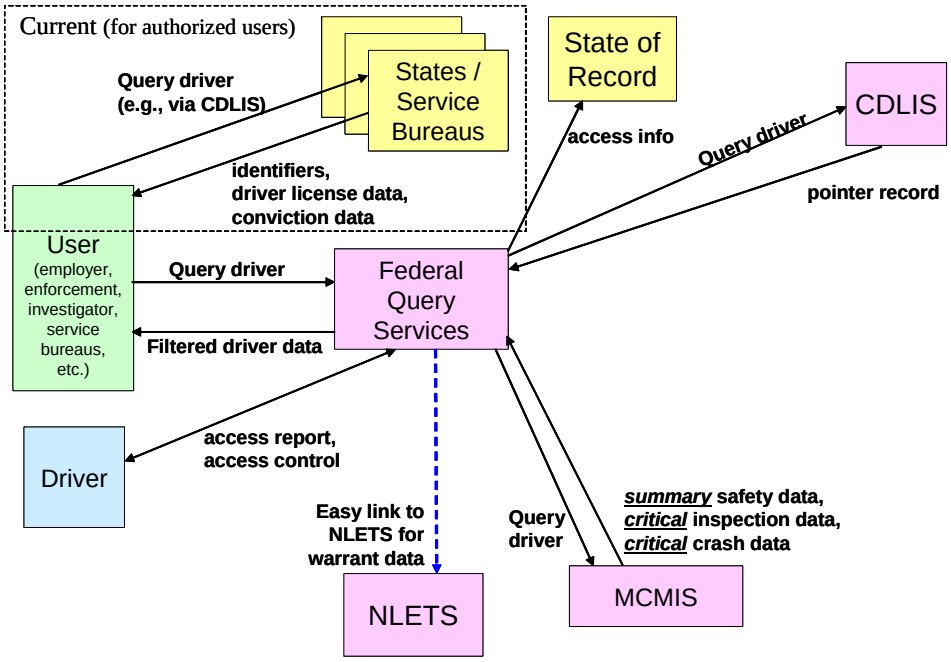

Figure 5-1. Option 1: Improve access to federally-held driver data

Under Option 1, the impact on MCMIS or a system that accesses MCMIS data would be substantial because those data are currently organized by carrier rather than by driver. The improved access to driver information would be managed according to business rules. Systems that support inspections, crash reporting, compliance reviews and medical waiver processing could be modified to query for background information. A common algorithm would be provided to determine driver safety scores. State systems would be changed to use the query service to support driver-related processes. Industry systems would be changed to take advantage of the improved access to federally-held data, but would continue to request license and conviction information from states or service bureaus.

5.2 Option 2: Provide a "full driver report" from federal systems

Today, FMCSA provides carrier safety profiles that summarize a carrier's national safety performance. Under Option 2, FMCSA would provide an equivalent thorough report for a commercial driver. The "Full Driver Report" would contain:

- Driver name, license ID, license jurisdiction
- Summary safety data
- Critical data from individual inspections
- Critical data from each federally-reportable crash report
- History of carrier associations as derived from inspections

- Individual crash report details for past 5 years
- Individual inspection reports for past 3 years.

This new/expanded federal capability would not provide:

- Current CDL status
- Conviction information
- Moving violations that are not related to an inspection.

This option differs from Option 1 in the scope of information available and the source system that would be responding to the request for information. Everything provided in the first option is part of this Full Driver Report. In addition, the full inspection reports and crash reports themselves would be provided. The Full Driver Report would be available to federal and state investigators, driver licensing agents, enforcement personnel, carriers, the driver, and potential employers. Users would register to be authorized to access the driver data. Drivers could control what private entities/people are able to access their records, and see who has accessed their records.

FMCSA would offer Full Driver Report request services so that users could request a full driver report and have that request managed by retrieving records from an analysis data warehouse. The data warehouse would contain copies of data reports stored in the production systems. Full Driver Report services would be provided based on user role and authentication. FMCSA would provide information only for drivers about whom data are held in FMCSA systems. Figure 5-2 illustrates the high-level architecture for this option.

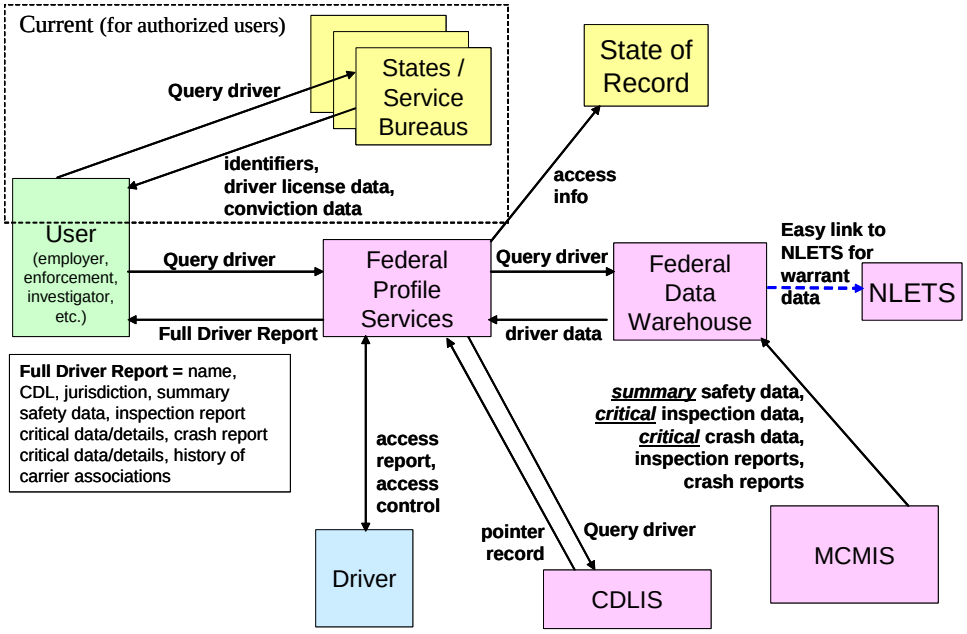

Figure 5-2. Option 2: Provide a "full driver report" from federal systems

5.3 Recommended Option 3: Provide facilitated centralized query

This option was originally described in the **Driver Snapshots** capability report. Since it really does not involve stored data, it is not a "snapshot" solution, and belongs in this report instead.

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. Drivers could control what private entities/people are able to access their records and see who has accessed their records. The central query service would interface with all necessary state and federal systems that are authoritative sources for driver snapshot information. The user or system that wants "snapshot" data would retrieve the data and integrate it as desired. Only the user or system that wants the snapshot might store the snapshot for later use. Figure 5-3 illustrates the high-level architecture for this option.

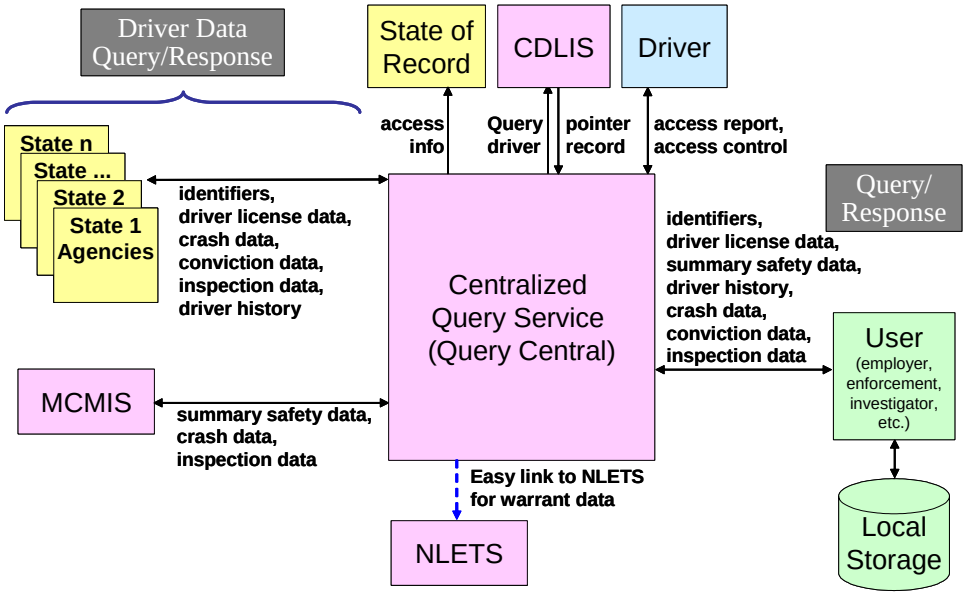

Figure 5-3. Recommended Option 3: Provide facilitated centralized query

Under this option, driver data would be retrieved from MCMIS for all inspections and crashes that are forwarded to MCMIS. Driver data associated with inspection and crash reports that are not forwarded to MCMIS would be retrieved from the appropriate state system. A common algorithm would be provided to determine driver safety scores. The scores would be computed by MCMIS for drivers about whom it has sufficient data. The safety ratings would be computed periodically. A link would be provided to enable easy access to National Law Enforcement Telecommunication System (NLETS) for authorized users. Many state systems would be changed to respond to the centralized query service for driver information. The centralized query service would provide standard data outputs and monitor and control access based on a user's role and authority. Automated processes would be required to reconcile data from different

sources and match records properly. Manual intervention might also be required. State systems might also be changed to use the centralized query service during driver licensing checks and to retrieve driver data for roadside operations. Industry systems would be changed to use the centralized query service.

5.4 Rejected Option: Augment CDLIS or driver licensing systems to access SAFETYNET

State driver licensing systems currently hold license and conviction information. State SAFETYNET systems hold inspection and federally-reportable crash data. For this option, the state driver licensing systems or CDLIS would be augmented to facilitate linking driver licensing records with driver Level III inspection and crash data from SAFETYNET. Via CDLIS, a user could request driver data and could receive license, conviction, inspection, and crash information.

Under this option, federal systems that support compliance reviews and medical waiver processing would query for driver data from the states. A common algorithm would be provided to determine driver safety scores. In addition to modifying the state driver licensing as described above, state roadside systems would be changed to request driver data when needed. CDLIS would be modified to handle additional data and could be modified to link to both driver licensing systems and SAFETYNET systems. Industry systems would be changed to use the additional data provided via CDLIS.

This option might also be adapted by commercial service providers to enhance their existing services.

This option was rejected because Option 3, “Provide facilitated centralized query”, would provide comparable functionality and has stronger technical and institutional merit. Neither CDLIS nor the state driver licensing systems currently interface with the SAFETYNET system.

6 Cost-Benefit Analysis

The following table provides a high-level cost-benefit analysis for each solution option identified in the previous section. Note that the options do not provide a common level of functionality.

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 information to authorized users or system
- Con: Incur significant costs to define, implement, and achieve standards for driver information sharing.

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 (Improved access to federally-held driver data)	All: Could summarize any driver data held in a FMCSA system. Could build on existing centralized system. Could focus on highest value data. Federal: Opportunity to integrate with and leverage the Creating Opportunities, Methods, and Processes to Secure Safety (COMPASS) initiative. Opportunity to integrate federal driver-related processes. State: One-stop shop for federally-held driver data. Industry: One-stop shop for federally-held driver data.	All: Data held only by states would still be accessed via the states. Federal: Requires increased access bandwidth. Significant changes to an existing system or new system development. State: --- Industry: Must still get state-held data from state or service provider.	Federal: not considered State: not considered Industry: not considered
2 (Provide a "full driver report")	All: Could share any driver data held in a FMCSA system. Could build on existing centralized system. Would provide rich source of federally-held information about drivers. Federal: Opportunity to integrate with and leverage COMPASS initiative. Opportunity to integrate federal driver-related processes. State: One-stop shop for federally-held driver data. Industry: One-stop shop for federally-held driver data.	All: Data held only by states would still be accessed via the states. Federal: Requires increased access bandwidth. Significant changes to an existing system or new system development. State: --- Industry: Must still get state-held data from state or service provider.	Federal: not considered State: not considered Industry: not considered

Option	Pro	Con	Cost
3 (Provide facilitated centralized query)	All: No additional data replication. Federal: Builds on Query Central and COMPASS initiative. No significant data storage. State: Centralized query service manages access control. No data push on change. Current data for roadside. Industry: Single interface; current data.	All: Response time may vary widely. Federal: Requires significant access bandwidth. Significant changes to an existing system or new system development. State: Must respond to queries from federal system. Roadside must query in real time (or else use potentially stale data from old query). Industry: ---	Federal: Medium State: Medium 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.

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. All three solution options provide improvements. Options 1 and 2 would provide better access to federally-held data; Option 2 may be more than some users need. Access to data about drivers who work only for intrastate carriers may be difficult to address with either Option 1 or 2. Option 3 should provide a level playing field in terms of access to data about all commercial drivers. Limiting the driver data to be shared should reduce costs. Choosing a solution that moves towards a realistic long-term vision in affordable increments will make the process more successful. Once the initial investments have been made to upgrade the systems that collect, store and use driver 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. 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

The recommended option proposed involves accessing information about drivers in systems that are currently centered on carriers or on the systems that provide the information. A fresh look would be required to organize the information based on how it is related and used rather than how it is collected. 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 about 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 Access to Driver Data 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 onboard technologies to improve on-road and roadside operations and reduce costs.

The working group recommends two activities related to this capability. The first activity focuses on determining an approach for a driver safety rating (please see the description in the **Driver Snapshots** capability report, reference 1). The second activity focuses on expanding the capabilities of Query Central (or its equivalent) to prototype the "Provide facilitated centralized query" option.

9.1 Driver Safety Rating Focus Group

Recent research should be examined for possible approaches to determining a driver safety rating. Please see the description of this activity in the **Driver Snapshots** capability report (reference 1).

9.2 Facilitated Centralized Query Prototype

A project should be developed to prototype the "Provide facilitated centralized query" option for the Access to Driver Data capability. The prototype should build on the existing Query Central capability to query for driver data via CDLIS and the ongoing prototype for retrieving additional data from inspection and crash reports stored in MCMIS. The prototype should include multiple states and enforcement users to assess the feasibility of a broader implementation. Several industry representatives should be involved in the prototype to evaluate the impact on service bureaus, large carriers, smaller carriers, and other stakeholders. Accessing information for interstate, intrastate, and foreign drivers should be included in the prototype. Drivers must be fairly represented on the project team, perhaps via the national or state chapters of the American Trucking Associations and/or via the Owner-Operator Independent Drivers Association. AAMVA has extensive experience in consensus building and information sharing where driver data are concerned and is willing and should be part of the project team. Landstar and the North Dakota State University Upper Great Plains Transportation Institute may also be interested in participating in this prototype.

10 References

1. JHU/APL, *Expanded CVISN Driver Information Sharing Capability Report: Driver Snapshots*, SSD-PL-05-0194, June 2005.