1 Capability

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

> Enhance interfaces and systems for information sharing to provide improved access to more current and accurate credentials information for authorized stakeholders.

2 Working Group Recommendations

The Expanded E-Credentialing Working Group offers these summary recommendations related to this capability:

- There are a number of items originally listed as Expanded Commercial Vehicle Information Systems and Networks (CVISN) in e-credentialing that are, in fact, prerequisites for successful e-credentialing and, therefore, are not part of Expanded CVISN. For CVISN to achieve the original core capabilities these issues must be successfully addressed.
  - The Federal Motor Carrier Safety Administration (FMCSA) must take the lead in coordinating with the entities charged with International Registration Plan (IRP) and International Fuel Tax Agreement (IFTA) registration and permitting to enable near real-time availability of data. Absent the availability of current data across the country, the use of these data in any screening operation will be counterproductive.
  - A single and unique number must be assigned to every carrier, and this must be a required field for all credentials. If this is to be the US Department of Transportation (USDOT) number, then the database of these numbers must be thoroughly cleansed to eliminate any multiple entries for single carriers.
  - A number of states will never succeed in deploying Core CVISN if they aren't provided the technical support needed to successfully implement CVISN-compliant e-credentialing. FMCSA should establish a technical support team, either internally or through a vendor with access to various technologies, that could be made available to states requiring this assistance.
  - States must be encouraged to fill the credentials-related fields in Safety and Fitness Electronic Records (SAFER) snapshots to enable credentials data sharing across jurisdictions.
  - States need to share Single State Registration System (SSRS) information. Consideration should be given to sharing SSRS data (or its replacement) via SAFER.
- We are concerned that the approach being taken by Expanded CVISN may not meet the needs of a changing environment. While the different working groups may be able to focus on a few key issues that exist today, these may not be the issues of highest priority a year from now or at any point in the future. As such, the Expanded E-Credentialing Working Group recommends that some portion of available funds be set aside to address

emerging issues. We further recommend that either this working group or some similarly-constructed group of representatives of CVISN-affected entities be reconstituted annually to review issues and develop priorities for e-credentialing.

- The working group recommends two options in this report:
  - Provide on-line access to Heavy Vehicle Use Tax (HVUT) payment status
  - Make SAFER provide better access to credentials data
- Two activities related to this capability are proposed for near-term funding, each tied to one of the recommended options:
  - Work with the Internal Revenue Service (IRS) to define an approach to allow on-line access to HVUT payment status via SAFER.
  - Prototype an enhanced version of SAFER to provide additional credentials data and real-time query/response via SAFER to authoritative credentials systems of record.
- The working group is also concerned about the apparent intent of FMCSA to concentrate available funds on two or three projects for development. It is our opinion that the activities needed to ensure that CVISN e-credentialing is a success require leadership and/or a commitment of administrative and technical support resources by FMCSA to achieve, and that the activities will not require a significant expenditure of Expanded CVISN resources. Therefore we urge FMCSA not to limit the number of Expanded CVISN initiatives to be undertaken.

3 Concept of Operations

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), SAFER, Commercial Vehicle Information Exchange Window (CVIEW), Performance and Registration Information Systems Management (PRISM), IRP and 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
- More timely and complete IRP and IFTA data in snapshots
- 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)
- Electronic security device event data (to track the status of and activities related to a security device attached to the container and/or trailer)
- Integrate with or link to asset tracking, arrival scheduling, and other vehicle, port and freight information systems [e.g., Freight Information Real-Time Systems for Transport (FIRST), electronic freight manifest, State On-Line Enforcement System (STOLEN)].
- Access to up-to-date credentialing information [e.g., oversize/overweight (OS/OW) permits].

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

- Open standards for data collection and reporting
- Access to driver snapshots
- Out-of-service (OOS) processing, to include automatically purging/updating expired OOS indicators
- Hours of service compliance evaluation
- 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 Communication (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)
- E-credentialing deployments (e.g., Core CVISN Web credentialing)
- Broader transportation infrastructure deployments (e.g., e-toll collection)
- Data sharing models (e.g., CDLIS)
- Border technologies and information flows [e.g., Automated Commercial Environment (ACE), International Trade Data System (ITDS)].

4 Requirements

Discussions with the members of the Expanded E-Credentialing Working Group established by FMCSA via the ITS/CVO 2005 Deployment Showcase seeded the requirements stated in this section. Subsequent review by members of the Expanded E-Credentialing Working Group finalized the requirements.

Access to credentials information is needed to:

- Validate that the credential is current. For example,
  - Verify HVUT payment status
  - Verify active IFTA registration
  - Verify IFTA payment status
  - Verify HazMat endorsement
  - Verify IRP registration

  - Verify OS/OW credential information, including authorized size, weight, and route
  - Verify SSRS status.

- Link information from different systems. For example,
  - Carrier as taxpayer linked with carrier as safety entity
  - Vehicle linked with vehicle registrant
  - Driver associated with carrier.

- Identify the responsible party. For example,
  - Identify who is responsible for a leased vehicle
  - Identify the carrier responsible for vehicle safety.

To improve access to credentials data, the data should be standardized in some ways:

- A unique standard identifier should be used for a carrier, vehicle, and driver in all records. Please see the **Safety Data Quality** capability report (reference 1) for more on this requirement.
- The data semantics (business meaning/intended usage) for every credentials data element that must be shared across jurisdictions and agencies should be common or at least made available to all users of the information.
- The data syntax (format/allowed range of values) for every credentials data element that must be shared across jurisdictions and agencies should be common or at least made available to all users of the information.

Sometimes similar data must be maintained in separate systems; for example, the contact name used by a carrier for tax purposes may differ from the contact name for safety purposes.

To issue a credential-related citation, enforcement personnel and systems require access to current credential information.

Access should be provided for this credentials-related information:

- Carrier: Identity, census (e.g., business identification, contact data, operation data, state-specific data), operating authority status/flag, SSRS status/flag, IRP status/flag, IFTA status/flag, insurance status/flag
- Vehicle: Identity, census (e.g., title, state-specific data), registration status/flag, registration weights/states/dates, permit characteristics and status, tax payment status/flag, whether plate matches cab card
- Driver: Identity, census (e.g., name, address, identifying information), driver license data, biometrics, OOS status
- Cargo: permit characteristics and status
- Trip: temporary credentials (e.g., OS/OW, HazMat).

To facilitate credentials information sharing, common structures and protocols should be established. The common structures and protocols would serve both people and automated information sharing via software systems.

Rules for accessing information about state-issued credentials differ according to state laws. In general, business information is shareable and personal information is not. Different access levels should be provided based on the data to be shared and different user types.

Access rules themselves should be published via open standards so that information systems can abide by them.

As much as possible, sharing information about interstate and intrastate operators should be handled the same way.

5 Potential Solution Alternatives

Several potential solution options for the **Access to Credentials Data** capability were identified. The working group decided that the options listed below are worth further investigation:

- Recommended Option 1: Provide on-line access to HVUT payment status
- Option 2: Provide facilitated centralized query
- Recommended Option 3: Make SAFER provide better access to credentials data.

The working group chose Options 1 and 3 as higher priority and preferred over Option 2 for improving access to credentials data. For each solution option, the architecture and possible impacts on federal, state, and industry systems/business processes are summarized.

In the Draft 2 report, five options were proposed. As a result of the April working group telecon, the group decided that the two “options” listed below should really be addressed as part of Core CVISN. They are now stated as recommendations in Section 2. For reference, the original discussion of each item remains in this section.

- Fill existing SAFER credentials data fields
- Ensure a single USDOT number is assigned to a carrier.

The working group decided that the following option is not worth pursuing:

- Establish access to individual systems of record that hold credentials data.

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 Recommended Option 1: Provide on-line access to HVUT payment status

As a condition of receiving federal highway funding, states are required to verify payment of HVUT prior to issuing an IRP credential. This has been problematic for electronic credentialing processes. The IRS does not enter vehicle information on HVUT receipts for fleets with more than 25 vehicles (although recent legislation requires the IRS to enter this information). In the past, there was no database to "hit" against to verify HVUT payments electronically.

Most states have developed work-arounds to enable e-credentialing for IRP, with subsequent verification of the paper HVUT receipt. However, this typically requires the state to revoke registrations if the paper verification is not provided after the fact. States would prefer to electronically verify that the HVUT payment is current at the time of credentials issuance. With passage of recent legislation, it appears that the IRS will be developing a database that could be used in electronic verification of HVUT payments. Recent interactions between FMCSA and the IRS on this subject have been promising. It is critical that those required to enforce restrictions based on HVUT payment infractions (e.g., state vehicle registration agencies) are able to learn whether or not a vehicle's HVUT payment status is good via electronic means.

Under this option, FMCSA would work with the IRS and states to provide on-line access to HVUT payment status. Access to other credentials data would remain as it is today under this option. Two approaches are suggested for consideration in providing on-line access to HVUT payment status. The working group prefers Option 1b.

- Option 1a: Develop a Web services query via Query Central or some other mechanism to enable person-to-system queries to verify HVUT payment at the time of vehicle registration (whether vehicle is being registered via e-credentialing or manual process); states could then use this standard query capability in their IRP processes. Roadside officers could also determine HVUT payment status via the query mechanism. Figure 5-1 illustrates this approach. Note that the figure also shows electronic payment of HVUT, not actually part of this capability, but a related concept.

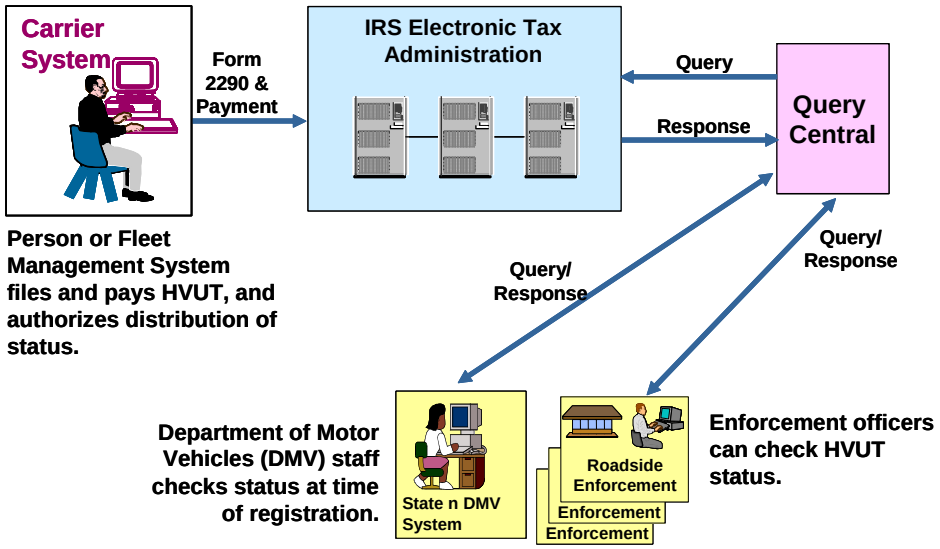

Figure 5-1. Option 1a: HVUT status via Query Central

- Preferred Option 1b: Routine download of HVUT payment status from the IRS database to SAFER, enabling states to download the required information from SAFER to their state CVIEW or CVIEW-equivalent, with the state developing required system-to-system queries from the IRP system to state CVIEW to enable electronic verification. Figure 5-2 illustrates this approach. Note that the figure also shows electronic payment of HVUT, not actually part of this capability, but a related concept. The working group prefers this option because states could use existing SAFER interfaces to access the information. The status information must be updated in a timely fashion to be of use.

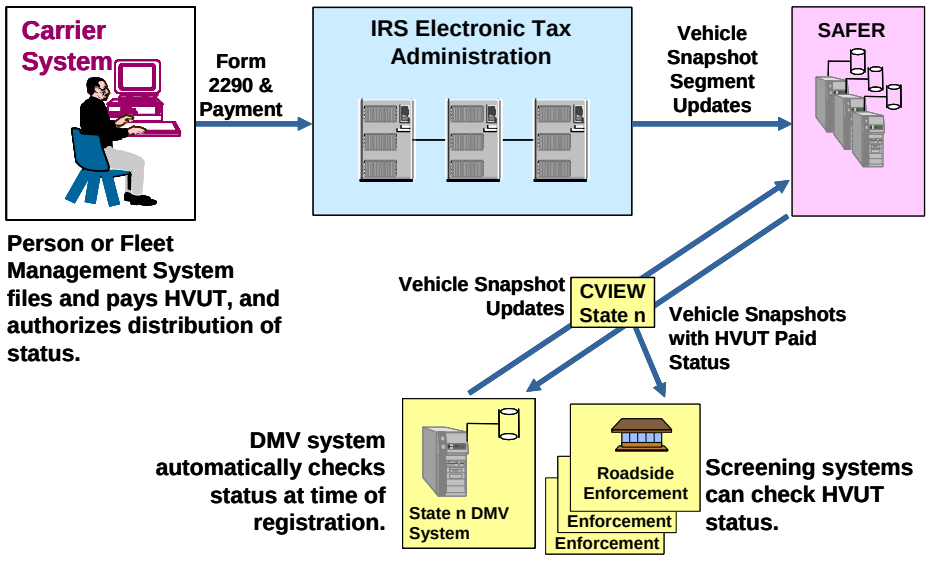

Figure 5-2. Preferred Option 1b: HVUT status via SAFER

5.2 Option 2: Provide facilitated centralized query

In this option, a centralized query service would be provided for all authorized users to gain access to credentials data. Query Central is a model. The central query service would interface with all necessary state and federal systems that are authoritative sources for credentials information. The user or system that wants credentials data would retrieve and integrate the data via the centralized service. Figure 5-3 illustrates the high-level architecture for this option.

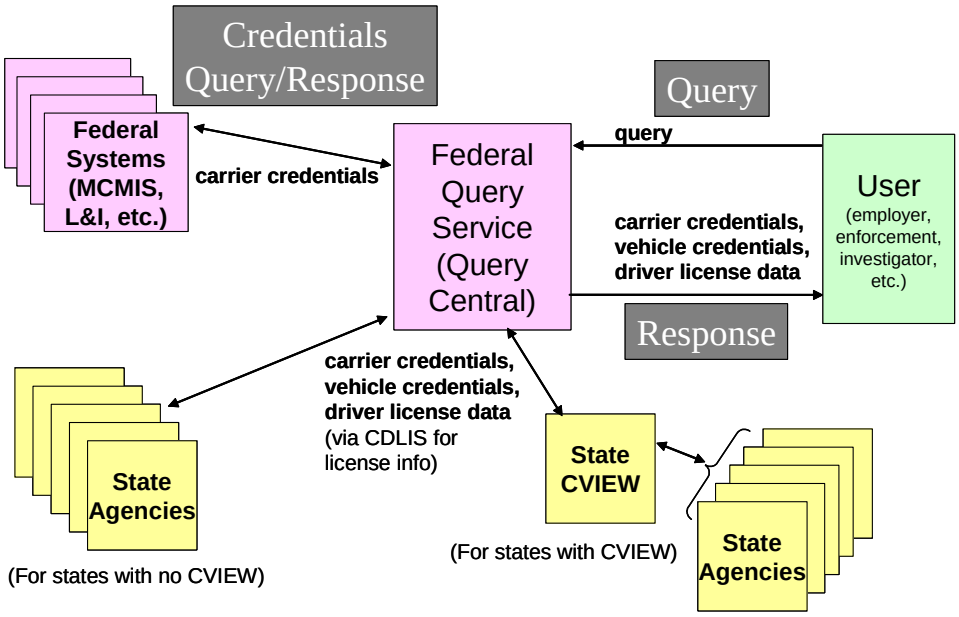

Figure 5-3. Option 2: Provide facilitated centralized query

Under this option, the facilitated centralized query system would retrieve driver data from state driver licensing systems via CDLIS. FMCSA-held carrier credential data would be retrieved from MCMIS and Licensing and Insurance (L&I), or their equivalent. The facilitated centralized query system would retrieve state-held vehicle and carrier credentials data either directly from state systems or via CVIEW. State systems would be changed if necessary to respond to the centralized query service (or CVIEW query) for credentials information. The centralized query service would provide standard data outputs and monitor and control access based on a user's role. State systems might also be changed to use the centralized query service during credentialing and roadside operations. Industry systems would be changed to use the centralized query service. Different access permissions would be granted based on a user's role (established during a registration process).

5.3 Recommended Option 3: Make SAFER provide better access to credentials data

SAFER was conceived to serve a multitude of purposes. To meet this capability's requirements, this option focuses on enhancing SAFER. Specific credentials data required by office, roadside, and carrier personnel would be added to the carrier, vehicle, and driver snapshots as needed. Subscription criteria and fulfillment processes would be re-evaluated to streamline the process of maintaining credentials data in the snapshots. Query/response mechanisms would be modified to allow real-time queries from users and systems via SAFER to authoritative sources of record. SAFER users would access all services through a single sign-on. Figure 5-4 illustrates the high-level architecture for this option.

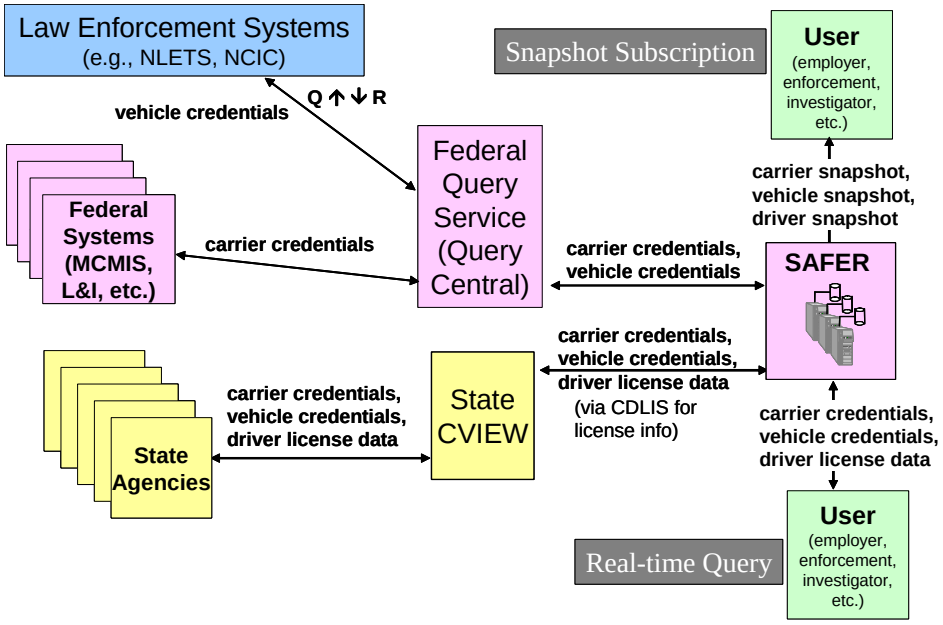

Figure 5-4. Recommended Option 3: Make SAFER provide better access to credentials data

Under this option, SAFER would be the federal system most affected. To facilitate real-time queries to federal data, SAFER would interface with Query Central. Data currently missing from SAFER snapshots would be pushed to SAFER by whatever system is the authoritative source. To facilitate real-time queries to state data, SAFER would interface with each state's CVIEW. CVIEW would interact with its own state's authoritative source credentials systems to retrieve the information requested in the query. If a state has not implemented CVIEW, it might be possible to connect the state credentialing systems directly to SAFER to provide access to credentials information. States would be encouraged to keep SAFER snapshots up to date so that their own systems have access to the best information possible. State systems could be changed to use SAFER snapshots as the primary source of information. Industry systems and users could be registered to access credentials information via SAFER.

For this solution to result in significantly improved access to credentials data, it must be adopted by all jurisdictions. An incomplete set of information in SAFER snapshots or spotty participation in the query/response process would continue the status quo rather than realizing the capability intended.

The working group suggests that a hybrid involving the facilitated centralized query solution for this capability (Option 2) and this solution should also be considered. Those who request credentials data via Query Central could be provided the appropriate data from the stored snapshot as a first response. If that information did not satisfy the user's need, a second query could be used to retrieve the additional information via SAFER/CVIEW/authoritative sources as shown in Figure 5-4.

5.4 Changed to recommendation to be addressed in Core CVISN: Fill existing SAFER credentials data fields

SAFER was designed to collect some credentials data and support roadside operations and credentialing processes. To meet this capability's requirements, this item should be considered an important part of Core CVISN that must be completed. Efforts should focus on motivating states to fill the existing SAFER credentials data fields so that all authorized users will be able to access the information routinely. The credentials data fields that exist in SAFER today include:

- From states:
  - IFTA account, name, and address
  - IRP account, name, and address
  - IRP fleet, name, and address
  - Vehicle Identification Number (VIN), registration, and proration information
  - Carrier e-screening authorization
  - Vehicle transponder information
- From MCMIS
  - Carrier, carrier classification, carrier cargo classification, and carrier HazMat information.

Please see SAFER documentation for details,
(http://cvisn.fmcsa.dot.gov/Documents/Document_Nav_Frame_Page_documents.shtml)

Transactions exist to upload and download the credentials information listed. If these existing fields were complete and current for all carriers, the SAFER database would contain much of the credential information required for carriers and vehicles at the roadside and by other authorized information users outside the home jurisdiction.

FMCSA should work with stakeholders to improve the routine, proactive upload of credential information to SAFER. Significantly improved access to credentials data would be provided if all jurisdictions routinely kept the existing credentials fields in SAFER snapshots up to date.

Incomplete information in SAFER snapshots will continue the status quo rather than realizing the Core CVISN capability intended.

5.5 Changed to recommendation to be addressed in Core CVISN: Ensure a single USDOT number is assigned to a carrier

Every motor carrier should have a unique identifier, preferably a USDOT number. Further, motor carriers should have only one USDOT number. Today a "carrier" sometimes has multiple USDOT numbers, which makes it difficult to associate data correctly with the carrier. PRISM states must verify the USDOT number of the carrier responsible for safety at the time of interstate vehicle registration. When the same carrier has more than one USDOT number, it becomes the state's "problem/headache" to sort through and clean this up. Note that this problem can be considered a data quality issue; please see the **Safety Data Quality** capability report (reference 1) for more on data quality issues. The working group determined that resolving this issue is a key element of Core CVISN that must be addressed.

Several factors contribute to a carrier having multiple USDOT numbers:

- Lack of a universal definition of what constitutes a "carrier." The definition is particularly confusing with leasing arrangements and where parent companies treat fleets as separate entities. In the latter case the parent companies often apply for and receive USDOT numbers based on terminal address and, therefore, end up with multiple USDOT numbers for a single Federal Employer Identification Number (FEIN) (e-mail from Don Baker, dbaker@dot.state.ny.us, 28 March 2005).
- Generally the corporate office or headquarters should file all the necessary forms and inform its branches of the USDOT number. In the past, there have been examples of giant companies with thousands of trucks being reduced (in the eyes of the FMCSA) to small operations with a handful of trucks and drivers just because a branch office filed a MCS-150 form in error. This causes problems when it is time to calculate safety ratings. (http://www.usdotnumberregistration.com/news.asp#ge4)
- Carrier that changes from intrastate to interstate operations. If the carrier already has a USDOT number, the company should not get a new one, but some may.
- Shipper that becomes a carrier. Again, if the company already has a USDOT number, it should not get a new one, but some may.
- Carrier with inactive USDOT number that wants to start to operate again. The carrier should follow procedures to activate the existing USDOT number, but some may apply for a new number.

FMCSA should work with states and industry to:

- Review the USDOT number issuance process to gain a better understanding of how multiple issuance occurs

- Clarify the definition of a carrier
- Ensure that a single USDOT number is assigned to a carrier
- Develop safeguards in the process to minimize the potential for issuance of multiple USDOT numbers to the same operator
- Provide clear direction to states for resolving problems.

Related to this issue is the idea that all records associated with a carrier should carry a unique carrier identifier (preferably the USDOT number) so that the information can be linked across systems and jurisdictions. For instance, today, not all IRP and IFTA registration/permit processes require that the USDOT number be recorded. If every carrier-related credentialing process required that the USDOT number be recorded, this would allow cross-referencing the credentials information with safety information. The PRISM process already requires that the USDOT number of the carrier responsible for the safety of the vehicle be recorded when the vehicle is registered. To resolve this issue, FMCSA should work with states and industry to:

- Establish a unique identifier for each carrier (interstate or intrastate, for hire or private), preferably the USDOT number
- Collect that unique identifier in all credentialing and safety operations (including IRP and IFTA processes) so that information related to the carrier can be cross-referenced across systems and jurisdictions.

5.6 Rejected Option: Establish access to individual systems of record that hold credentials data

Different systems store credentials data. Systems include those that manage carrier registration, driver license information, vehicle registration, vehicle titling, tax registration, tax collection, and permitting information. In this option, these systems would be modified to allow access for all legitimate users of credentials information. The user or system that wants credentials data would retrieve and integrate the data.

Under this option, the impact on federal systems would be minimal, since access to federal credential information is already provided via existing systems. Many state systems would be changed to enhance access to credentials information, provide standard data outputs, and monitor and control access based on a user's role. State systems might also be changed to access other states' systems for credentials checks and to retrieve 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.

6 Cost-Benefit Analysis

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

- Improved access to credentials information
- Improved ability to target enforcement resources
- Improved safety, security, and productivity.

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 (Provide on-line access to HVUT status)	All: --- Federal: More tax revenue for Highway Trust Fund. State: Reduced burden to comply with federal regulations. Industry: Improved customer service.	All: --- Federal: Changes to IRS and FMCSA systems required. State: Changes to state processes/systems required. Industry: ---	Federal: Low to Medium State: Low Industry: Low
2 (Provide facilitated centralized query)	All: Same interface for all queries. Federal: Builds on Query Central and Creating Opportunities, Methods, and Processes to Secure Safety (COMPASS) initiative. No significant data storage. State: Let the centralized query service manage access control. No data push on change. Current data for roadside. Industry: ---	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 use data from old query. Industry: ---	Federal: Medium State: Medium Industry: not applicable

Option	Pro	Con	Cost
3 (Make SAFER provide better access to credentials data)	All: Builds on existing systems to improve information sharing. Federal: Leverages SAFER and Query Central capabilities. State: If CVIEW can already interface with authoritative source systems, impact should not be major. Industry: Access to current data.	All: --- Federal: --- State: If CVIEW and credentialing systems not set up for query/response handling, impact may be significant. Industry: ---	Federal: Medium State: Medium Industry: not applicable

7 Business Case

Some jurisdictions have made progress in sharing IRP data via CVIEW/SAFER. However, too few are providing full data sets to SAFER to support CVO credentialing processes and roadside enforcement activities. The CVISN infrastructure has demonstrated the effective exchange of credentials data, with orderly and traceable change processes to accommodate discovered problems. Credentialing processes are not coordinated across jurisdictions, agencies and programs, requiring redundant data entry that is tedious and error-prone. Terminology and data definitions are not always consistent. Validation of submitted data is problematic.
The technology to replicate information in a common database and share that information is available. CVIEW and SAFER have successfully shared information across agencies and jurisdictions. Realizing improved access to credentials data nationwide will be difficult because of the number of agencies and systems involved and because information standards are embryonic at best. Some states have successfully shared credentials data across agencies and with other jurisdictions, and can make the case for benefits realized.

8 Issues

8.1 Institutional Issues

Since existing systems do not all use the same identifier for carrier and vehicle, effort must be applied to enlist cooperation across agencies and jurisdictions to adopt common identifiers. Privacy statutes inhibit sharing some credentialing-related information. Revenue agencies are often reluctant to share tax information. Access to credentials information must be controlled accordingly. By agreement, some agencies can access other agencies' information, but those agreements may not extend to other users. It will be necessary to define what information can be shared by different types of users and establish some common means of enforcing the access rules. Some credentialing processes require similar information, but data definitions are not

standardized. What identifies a carrier for one credential may be different from the identifier for another credential (e.g., IRP and IFTA). States are required to verify HVUT payment status but do not have on-line access to the information from the IRS. The association of one entity with another may change, making it difficult to connect credentials and safety information (e.g., a driver may switch employers, or a vehicle may be leased to a second carrier during seasonal operations). While it is desirable to provide equal access to credentials information about interstate and intrastate operators, some business processes and credentials differ.

8.2 Technical Issues

The absence of common identifiers and data definitions creates technical barriers to improving access to credentials data. The technology to share credentials information is readily available and already implemented in states that have completed Core CVISN implementation.

9 Deployment Strategy

In deploying the **Access to Credentials 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 with the ability to challenge and correct their own census, inspection, crash, and citation information.
- Control access to sensitive information.

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.

The working group recommends two activities related to the Access to Credentials Data capability. The first activity involves working with the IRS to define an approach to allow on-line access to HVUT payment status. The second activity is to extend SAFER to provide improved access to credentials data.

9.1 On-line Access to HVUT Payment Status

A task force should be established to work with the IRS to define the requirements and approach for providing on-line access from state commercial vehicle registration offices to HVUT payment status. As described in Option 1b, the working group suggests that it would be most efficient for the states to build upon the SAFER model and retrieve HVUT payment status via SAFER snapshots or a query to SAFER. The task force should include representatives from the IRS, FMCSA, the SAFER team, industry, and state vehicle registration administrators. If there is a need for roadside enforcement to access the HVUT status as well, then roadside enforcement personnel should also participate in the task force. Once the requirements and approach have been agreed upon, a prototype should be planned to test the approach on a small scale.

Arkansas, Connecticut, Idaho, Kansas, New York, and Washington expressed interest in participating in this activity.

9.2 SAFER Access for Credentials Data

SAFER today has fields for some credentials data, and one of the earlier recommendations is to encourage jurisdictions to routinely fill those snapshot data fields. The requirements for accessing credentials data go beyond the existing SAFER capabilities in two ways: additional data and real-time access to information from the authoritative sources. For this activity, a single state or small group of states would work with the SAFER team to:

- Extend the SAFER snapshots to hold additional credentials fields
- Allow real-time queries from users and systems via SAFER to authoritative sources of record for credentials data.

The team should include interested states, the SAFER team, enforcement, and industry. As described in the general deployment strategy section earlier, the prototype team should consider implementing a small-scale solution that can be expanded or serve as a model for national deployment.

Arkansas, Idaho, Kansas, New York, South Dakota, and Washington expressed interest in participating in this activity.

10 References

1. JHU/APL, *Expanded CVISN Enhanced Safety Information Sharing Capability Report: Safety Data Quality*, SSD-PL-05-0196, June 2005.