

**AUDIT OF THE DATA INTEGRITY OF THE
COMMERCIAL DRIVER'S LICENSE
INFORMATION SYSTEM (CDLIS)**

Federal Motor Carrier Safety Administration

Report Number: FI-2009-067

Date Issued: July 30, 2009



Memorandum

**U.S. Department of
Transportation**
Office of the Secretary
of Transportation
Office of Inspector General

Subject: ACTION: Report on the Audit of the Data
Integrity of the Commercial Driver's License
Information System
Report Number: FI-2009-067

Date: July 30, 2009

From: Rebecca C. Leng 
Assistant Inspector General for Financial and
Information Technology Audits

Reply to
Attn. of: JA-20

To: Acting Deputy Administrator,
Federal Motor Carrier Safety Administration

This report presents the results of our audit of the data integrity of the Commercial Driver's License Information System (CDLIS), as required by the Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (SAFETEA-LU). The Federal Motor Carrier Safety Administration (FMCSA), a component of the Department of Transportation (DOT), is responsible for oversight of CDLIS.

SAFETEA-LU required that we perform a baseline audit that includes an assessment of the validity of the data in CDLIS and an analysis of the revenues derived from the use of CDLIS. SAFETEA-LU also required the Secretary to develop and publish a comprehensive national plan to modernize CDLIS that complies with applicable Federal information technology standards. Last summer, we issued a report presenting our analysis of derived revenues.¹ This report primarily addresses the validity of CDLIS data and security issues. Accordingly, we assessed (1) whether convictions received from the courts were recorded in a timely manner, (2) whether CDLIS and state department of motor vehicles (DMV) systems were adequately secured, and (3) the adequacy of contingency plans to ensure continued CDLIS service to DMVs following a disaster or other emergency.

¹ *Use of Income Derived from the Commercial Driver's License Information System for Modernization*, Report Number MH-2008-059, July 10, 2008. OIG reports are available on our website: www.oig.dot.gov.

To address our objectives, we tested a statistical sample of licensed commercial drivers having convictions; and we visited nine state DMVs and interviewed key officials concerning the sampled items, system security, and contingency planning. Our work also included interviews with FMCSA personnel and contractors, as well as reviews of technical documentation and departmental policy. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Exhibit A provides further details of our scope and methodology.

BACKGROUND

The Office of Inspector General (OIG) issued reports on the Commercial Driver's License (CDL) Program in 2000, 2002, and 2006.² The first report focused on the disqualification of commercial drivers, noting that out-of-state convictions were not transmitted to licensing states in a timely manner. This report also concluded that states did not disqualify commercial drivers, as required by law, and granted licenses to commercial drivers who posed a safety risk. The 2002 and 2006 reports focused predominantly on fraudulent licensing. Last year, as mentioned, we reported on the use of income derived from CDLIS for system modernization, as required by SAFETEA-LU. These reports contain recommendations to improve CDL program oversight.

Congress found that one of the leading factors operating against commercial motor vehicle safety was the possession of multiple licenses by commercial drivers. Drivers with multiple licenses spread their traffic violations over a number of state licenses to maintain a good-driver rating, regardless of the number of violations they acquire in one or more states. In response to states' concerns, the Commercial Motor Vehicle Safety Act of 1986 (CMVSA) directed DOT to establish minimum standards for licensing, testing, qualification, and classification of commercial drivers. CMVSA also prohibited commercial drivers from possessing more than one commercial license. The goal of CMVSA was to improve highway safety by removing unsafe and unqualified drivers from the highways, including ensuring that drivers of large trucks and buses were qualified to operate those vehicles.

² *Disqualifying Commercial Drivers*, Report Number MH-2000-106, June 30, 2000; *Improving Testing and Licensing of Commercial Drivers*, Report Number MH-2002-093, May 8, 2002; and *Oversight of the Commercial Driver's License Program*, Report Number MH-2006-037, February 7, 2006.

CMVSA further required that the Secretary of Transportation establish a nationwide information system for exchanging driver-related data among the states. CDLIS, administered by the American Association of Motor Vehicle Administrators (AAMVA) under a memorandum of understanding with FMCSA, was developed to meet this mandate. CDLIS is a central database that stores each commercial driver's name, date of birth, Social Security number, and the jurisdiction in which the driver is licensed (state of record). Currently, CDLIS maintains this information for about 13 million active and inactive commercial drivers. CDLIS does not contain driver histories itself; rather, it directs such inquiries to the state of record. This history should contain all driving convictions an applicant may have. Completeness of this information depends on the courts' providing DMVs with accurate conviction data, and DMVs' timely updating of their driver histories.

State officials use CDLIS to connect with other state DMV systems to check an applicant's driving history prior to issuing a commercial driver's license. In addition, CDLIS is accessed by about 5,000 state inspectors to perform roadside inspections; they gain access to CDLIS through a Web application system developed by FMCSA called *CDLIS-Access*.

RESULTS IN BRIEF

FMCSA has taken measures to strengthen the CDL program, but additional action is necessary to increase the safety of the Nation's highways. First, DMVs are still experiencing delays in posting convictions to their driver history records for CDLIS users' access. This continues to impede DMVs' ability to suspend or revoke problem drivers' commercial-driving privileges in a timely manner. Second, FMCSA and state DMVs have implemented password security measures to prevent unauthorized access to driver records and privacy information. However, deficiencies in security controls persist. Specifically, system certification and accreditation reviews³ have not been completed, and states lag in developing and implementing comprehensive security policies and procedures to better protect DMV systems. Third, enhanced contingency planning and testing of both CDLIS-Access and state DMV systems—to ensure uninterrupted CDL services after an emergency—has not fully occurred. As a result, users of these systems are vulnerable to service disruption. We are making a series of

³ Certification and accreditation reviews seek to provide assurance that systems are using the proper security controls to ensure adequate protection of the data they maintain.

recommendations, beginning on page 7, to improve the timeliness of conviction posting, CDLIS system security, and contingency planning.

STATES ARE NOT POSTING COMMERCIAL DRIVER CONVICTIONS IN A TIMELY MANNER

Our sample indicates that there are an estimated 500,000 active commercial drivers with out-of-state convictions for the 50 states and the District of Columbia. We focused on this group specifically because CDLIS is the primary method by which conviction data are sent between states. Based on our sample (253 randomly-selected drivers with convictions across nine states), we project that 20 percent of the active CDL-holders (99,000) had convictions that were not posted within the time frames established by FMCSA regulations.⁴

While some states in our review have taken action in an attempt to mitigate posting delays, such as automating the electronic interchange of data between courts and DMV, delays in courts' data submissions remain problematic. According to state representatives, late receipt of convictions from courts prevents them from posting conviction data within FMCSA's time frames. As a result, at the time of license issuance or renewal, DMVs may not have all information available with which to make an informed decision on whether a license should be granted, thereby possibly permitting an unqualified driver on the road. In addition, without a complete driver conviction history, DMV systems would not be able to provide information needed to effectively enforce Federal regulations to ensure that a driver's commercial license is suspended or revoked for a specific traffic conviction.

CDLIS AND SOME STATE SYSTEMS ARE NOT ADEQUATELY PROTECTING DRIVER DATA

Neither FMCSA nor AAMVA has entirely fulfilled its responsibility of securing the systems that house conviction data on America's commercial drivers—the

⁴ Beginning on September 30, 2005, notification to another state of traffic violations was required within 30 days of conviction. States must post a conviction to a driver history record within 10 days of the conviction if it occurred in the same state (49 C.F.R. § 384.225(c)), or within 10 days of receipt of the notice of conviction if it is from another state (49 C.F.R. § 384.209(c)). Information on some drivers within the sample was missing. For example, the date that the conviction record was added to DMV driver history was not always present, therefore restricting our analysis of timeliness. We estimate with 90-percent confidence that 15 percent of current CDL-holders have missing information in CDLIS, or about 75,000 out of an estimated 500,000. (Margin of error for estimates is +/-5 percentage points for current CDL-holders with out-of-state convictions, and +/-14 percentage points for not posting current CDL-holder convictions in a timely manner and for current CDL-holders with missing information.)

individuals entrusted with the safe conveyance of our trucks and buses. In addition, some of the states we visited have likewise not entirely fulfilled this responsibility.

FMCSA has not enforced the CDLIS-Access requirement that systems be accredited as adequately secured, nor has it included CDLIS-Access in its systems inventory. The Office of Management and Budget (OMB) requires that systems be inventoried and authorized (i.e., accredited) as adequately secured before beginning or significantly changing system processing, and reauthorized at least once every 3 years.⁵ Yet the contractor managing CDLIS-Access—used by state inspectors and FMCSA personnel to access state DMV commercial-driver records—was unaware that this requirement existed. In addition, we were unable to locate any contract provision that required the contractor to certify or accredit CDLIS-Access. We found two weaknesses in CDLIS-Access that could have been identified in the accreditation process: (1) user names and passwords were being transmitted without encryption, and (2) the Web site was vulnerable to certain hacker attacks.⁶ As a result, CDLIS-Access has increased exposure to intrusion.

Further, FMCSA has recognized the need to implement Federal security standards for CDLIS and has signed a memorandum of understanding with AAMVA (dated June 2008) requiring certification and accreditation of the system. However, no completion date was specified in the agreement, and to date, certification and accreditation have not been completed. Until completion of proper certification and accreditation, FMCSA will continue to lack a crucial management control to ensure that systems are properly assessed for security risk, have been independently tested, and that weaknesses have been identified and sufficiently mitigated. According to FMCSA management, they are working on the certification.

On the state level, for five of the nine DMVs in our sample, security policies were either nonexistent or had not been finalized. Federal laws, regulations, and guidance provide for the development of security policies to protect the confidentiality, integrity, and availability of data. While recognizing state sovereignty and that Federal requirements are not mandatory upon state DMVs, it would be prudent for states to develop and enforce an information security program. State officials reported that they had not developed comprehensive security policies due to a lack of resources, changes in separation of system responsibility between the state and DMV, and the absence of an established state-level approach to security requirements. Regardless, without adequate and

⁵ *Security of Federal Automated Information Resources, Circular A-130, Appendix III*, February 8, 1996.

⁶ We shared specifics of these vulnerabilities with FMCSA during the audit to facilitate its corrective actions.

comprehensive information security policies, states cannot establish or maintain an effective information security program that provides direction to users, enforces compliance, and ensures that security risks are reduced in a cost-effective manner.

FMCSA AND STATE DMVs LACK COMPREHENSIVE CONTINGENCY PLANS AND EVIDENCE OF TESTING

FMCSA does not have a contingency plan for CDLIS-Access, nor has it ever conducted a disaster recovery exercise for this system. According to the National Institute of Standards and Technology (NIST), effective contingency planning and testing are essential to mitigating the risk of system and service unavailability.⁷ While FMCSA management cites funding constraints, it is incumbent upon managers to allocate resources needed to implement departmental requirements. Until a contingency plan has been developed and tested, no assurance exists that users of this system—about 5,000 state roadside inspectors and 900 FMCSA personnel—will have timely access to state DMV CDL records in the event of a disaster.

Similarly, of the nine sample states reviewed, five could not provide contingency plan documentation or evidence that testing had been performed to ensure that their licensing systems could be recovered following a disaster. DMV officials cited prioritization of needs, changes in separation of system responsibility between state and motor vehicle administrations, and lack of standardized state requirements as reasons. In addition, according to these officials, the loss of use of their systems would have limited impact on their operations because they could revert to manual processing or even suspend issuance of licenses. Still, without viable and tested contingency plans, states may be unable to provide timely and complete conviction data to other states in the event of a severe or extended disruption, prolonging the period during which unsafe drivers may remain on the road.

CONCLUSIONS

Safety is the top priority of the Department of Transportation. Ensuring that convictions are posted in a timely manner would improve safety by enabling or facilitating timely removal of problem drivers from our highways. This will be more successful as CDLIS and DMV systems are better secured and system

⁷ *Contingency Planning Guide for Information Technology Systems, Special Publication 800-34*, June 2002.

contingency planning and testing become realities. Yet improving safety must be a cooperative venture between and among all stakeholders, including states, courts, the Federal Government, and partners such as AAMVA. And while efforts to improve safety through better oversight and coordination continue as CDLIS is modernized, it will be important to balance such actions against the necessity of securing driver privacy.

RECOMMENDATIONS

We recommend that the Acting Deputy Administrator, FMCSA, direct the Associate Administrator for Enforcement and Program Delivery to:

Timeliness of Posting of Convictions:

1. Require action plans from states to address tardiness in posting of convictions. Such plans should identify specific state problems in dealing with the courts, suggest solutions to these problems, and time frames by which the problems will be resolved or mitigated.

Security Policies and Procedures:

2. Complete the certification and accreditation of the CDLIS-Access system and add it to the FMCSA and DOT system inventories.
3. Implement, in conjunction with the FMCSA Chief Information Officer (CIO), a proper encryption mechanism on CDLIS-Access to protect user credentials while data are in transit.
4. Correct, in conjunction with the FMCSA CIO, the intrusion vulnerabilities in CDLIS-Access.
5. Require AAMVA to complete the certification and accreditation of CDLIS as required by the memorandum of understanding between FMCSA and AAMVA.
6. Promote and communicate to DMVs the need to establish security policies and procedures for safeguarding CDL information as part of CDLIS modernization.

Contingency Planning and Testing:

7. Prepare, in conjunction with the FMCSA CIO, contingency plans for CDLIS-Access, in accordance with OMB and NIST guidance.

8. Perform, in conjunction with the FMCSA CIO, disaster recovery testing of the CDLIS-Access system.
9. Promote and communicate to DMVs the need to perform periodic contingency testing for their licensing systems.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

We provided FMCSA with our draft report on June 8, 2009, and received its response on July 22, 2009. FMCSA concurred with all nine recommendations and discussed appropriate planned actions and target completion dates. FMCSA's response is included in its entirety in Appendix A.

ACTIONS REQUIRED

Management actions taken and planned are responsive to our recommendations, and are considered resolved subject to follow-up provisions in DOT Order 8000.1C.

We appreciate the courtesies and cooperation of representatives from the Federal Motor Carrier Safety Administration, and state DMV personnel who participated during this audit. If you have any questions concerning this report, please call me at (202) 366-1407 or Louis King, Program Director, at (202) 366-4350.

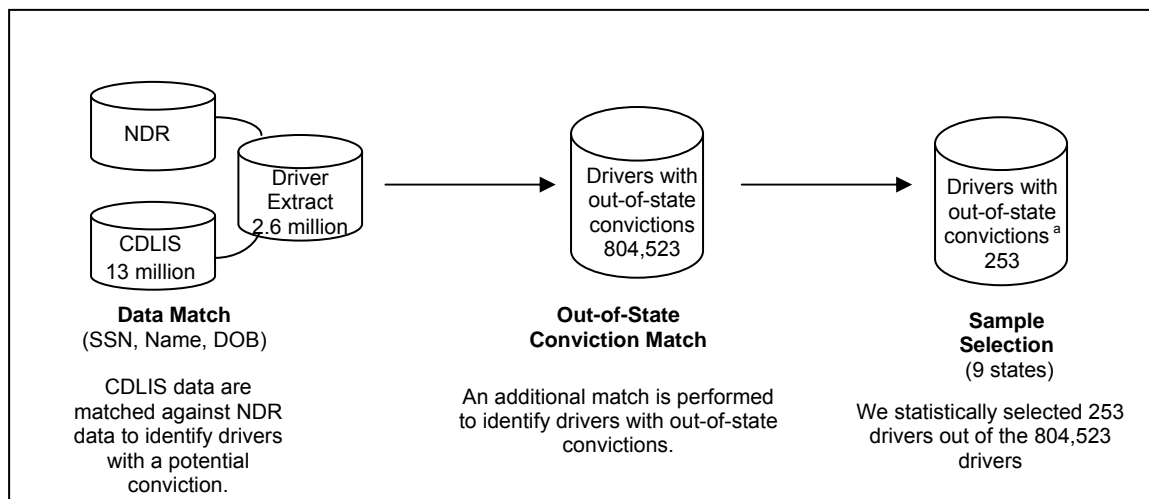
#

cc: Chief Information Officer, DOT
Martin Gertel, M-1
Karen Lynch, MC-TRS

EXHIBIT A. SCOPE AND METHODOLOGY

CDLIS is an archival database containing Social Security numbers, dates of birth, names, drivers' license numbers, states of record, and aliases for about 13 million commercial drivers. These records identify active or expired commercial driver's license (CDL)-holders, drivers applying for CDL licenses, and drivers convicted of driving a commercial vehicle without a valid commercial driver's license. In order to identify, to the extent possible, the number of individuals holding an active CDL who also had one or more traffic convictions, we matched CDLIS drivers to the National Driver Register (NDR).⁸ From this match, we selected a statistically valid sample in two stages. In stage 1 we selected nine out of 51 jurisdictions (the 50 states plus the District of Columbia) and in stage 2 we selected 253 out of 804,523 commercial drivers with out-of-state convictions. The nine states selected were California, Massachusetts, Mississippi, Missouri, New Jersey, New York, Oklahoma, Tennessee, and Texas. The figure depicts this process.

Figure. Selection of Commercial Drivers with Convictions from Other States



^a Drivers with out-of-state convictions were chosen specifically as CDLIS is the primary method of exchanging conviction data between states. (Source: OIG)

We made site visits to the nine states from May through July 2008 to determine the timeliness of processing conviction data for each driver in our sample. To address timeliness, we analyzed all convictions for each driver's history record from 2005 through 2008 and compared the time it took from the date of conviction

⁸ NDR is a central register that enables state DMV officials to exchange information on problem drivers in each state.

reported by the court to the date that the conviction was posted to the driver's record by the DMV. We conducted detailed observations, discussions, and reviews of policies and practices for the processing of traffic convictions, transmission of information to other states, problem resolution, and security controls established for protection of driver data. In each of the states we also compared specific Federal CDL regulations with the states' internal policies and practices for processing conviction data.

To assess the integrity of the state's system, we reviewed the CDL oversight practices, focusing on those relating to computer issues, by interviewing FMCSA officials and state CDL program officials at state offices, and reviewing documentation including CDL program reviews, correspondence between FMCSA and state officials, status reports from states to FMCSA on unresolved compliance issues, and other related documentation. Additionally, we assessed the integrity of the DMV system controls in processing the convictions by specifically focusing on the translation of state-of-record conviction codes to uniform Federal codes, and ensuring that this was being done accurately.

To address our objective on security, we used NIST security guidance as our baseline for best practices. While recognizing state sovereignty and that Federal requirements (including NIST's) are not mandatory upon state DMVs, it would be prudent for states to develop and enforce an information security program. We reviewed the state's information system security control policies and procedures; observed controls in operation (which included selecting a judgmental sample of items); and held discussions with officials at the state data center and motor vehicle administration to determine whether controls were in place, adequately designed, and operating effectively. Finally, we reviewed the information security practices at the contractor sites to assess whether they were consistent with Federal certification and accreditation requirements.

The audit work was performed between December 2007 and July 2008. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

EXHIBIT B. MAJOR CONTRIBUTORS TO THIS REPORT

<u>Name</u>	<u>Title</u>
Louis C. King	Program Director
Michael Marshlick	Project Manager
Michael P. Fruitman	Writer-Editor
Atul Darooka	Information Technology Specialist
Anthony Cincotta	Information Technology Specialist
Martha Morrobel	Information Technology Specialist

APPENDIX A. MANAGEMENT RESPONSE




Memorandum

U.S. Department
Of Transportation

**Federal Motor Carrier
Safety Administration**

Subject: INFORMATION: Response to the OIG Draft Report “Audit of the Data Integrity of the Commercial Driver’s License Information System (CDLIS),” 08F3003F000 **Date:** JUL 22 2009

From: 
Rose A. McMurray
Acting Deputy Administrator **Reply to Attn: of** MC-PRS

To: Rebecca C. Leng
Assistant Inspector General for Financial and
Information Technology Audits

The Federal Motor Carrier Safety Administration (FMCSA) reviewed the Office of Inspector General (OIG) draft report “Audit of the Data Integrity of the Commercial Driver’s License Information System (CDLIS)” and concurs with the recommendations. The commercial driver’s license (CDL) program supports the Agency’s mission by ensuring that only qualified and safe drivers operate commercial motor vehicles and continuously identifies the most effective strategies for improving driver safety. Based on the 2008 statistics recently released by the National Highway Traffic Safety Administration, the number of overall traffic fatalities reached its lowest level since 1961. Similarly, an early estimate of motor vehicle fatalities for the first quarter of 2009 shows that this favorable trend has continued into the current fiscal year. Large truck fatalities were down more than 12 percent in 2008 from 2007, and the large truck fatality rate per total vehicle miles of travel reached the lowest level ever recorded.

The FMCSA implemented several measures to strengthen the CDL program, and additional refinements related to CDLIS data, security, and modernization are in progress. It should be noted, however, that the Agency has limited authority to mandate Federal information technology security standards for the States. Further, the Agency must coordinate with 51 jurisdictions that do not have uniform traffic violation standards, unified court systems, standard electronic reporting methods, or statutes mandating the 10-day requirement for reporting CDL conviction data. The Agency is continuing to work with the States to address these challenges and strengthen CDL program oversight.

RECOMMENDATIONS AND RESPONSES

Appendix A: Management Response

RECOMMENDATION 1: Require action plans from states to address tardiness in posting of convictions. Such plans should identify specific state problems in dealing with the courts, suggest solutions to these problems, and time frames by which the problems will be resolved or mitigated.

RESPONSE: *Concur. As part of FMCSA's comprehensive CDL Compliance Reviews, States are required to submit corrective action plans to the Agency to address challenges, including meeting the timeliness requirement. Beginning in FY 2010, the Agency will provide each State with a quarterly report reflecting its compliance with the timeliness requirement, and a comparison with the other States.*

The Agency will also communicate to States the importance of achieving compliance with the timeliness requirement during the CDL Information Technology (IT) Users Workshop, scheduled for September 2009, and the CDL Coordinators Meeting, tentatively scheduled for February 2010. Written guidance is being developed, and will be available in September 2009 on the FMCSA and American Association of Motor Vehicle Administrators (AAMVA) web sites.

RECOMMENDATION 2: Complete the certification and accreditation of the CDLIS-Access system and add it to the FMCSA and DOT system inventories.

RESPONSE: *Concur. The Agency is currently reviewing the certification and accreditation (C&A) package for the CDLIS-Access system, which is hosted by a contractor, and anticipates adding it to the FMCSA system inventories by the end of FY 2009. The FMCSA informed the contractor that the CDLIS-Access system will be monitored by FMCSA, and must meet the requirements of the Office of Management and Budget Circular Number A-130, Management of Federal Information Resources.*

RECOMMENDATION 3: Implement, in conjunction with the FMCSA Chief Information Officer (CIO), a proper encryption mechanism on CDLIS-Access to protect user credentials while data are in transit.

RESPONSE: *Concur. The FMCSA directed its contractor to implement a proper encryption mechanism to protect user credentials. The contractor has initiated the purchase of a third-party digital certificate to meet encryption requirements, and will reconfigure the information system to utilize the protocol for encrypting web authentication traffic by the end of FY 2009.*

RECOMMENDATION 4: Correct, in conjunction with the FMCSA CIO, the intrusion vulnerabilities in CDLIS-Access.

RESPONSE: *Concur. By incorporating CDLIS-Access into the FMCSA Information System Continuous Monitoring Program, FMCSA's contractor will be required to report to FMCSA the status of remediation activities on emerging cyber threats and vulnerabilities. By the end of FY 2010, FMCSA will initiate weekly application and vulnerability scans on the CDLIS-Access information system. The FMCSA Information System Security Officer (ISSO) and the contractor will review scan result reports and deploy recommended fixes.*

RECOMMENDATION 5: Require AAMVA to complete the certification and accreditation of CDLIS as required by the memorandum of understanding between FMCSA and AAMVA.

RESPONSE: *Concur. The FMCSA will continue to work with AAMVA to ensure that C&A activities are accomplished in a timely manner. The AAMVA is currently on target to complete the C&A of CDLIS by the end of calendar year 2009. Additionally, FMCSA and AAMVA have recently agreed on an independent certification agent that will perform testing in accordance with commercial and Federal standards. The certification agent will evaluate the operational, management, and technical security requirements to determine the extent to which the controls are properly implemented, are operating as intended, and meet the system security requirements.*

RECOMMENDATION 6: Promote and communicate to DMVs the need to establish security policies and procedures for safeguarding CDL information as part of CDLIS modernization.

RESPONSE: *Concur. The FMCSA CDL Division, FMCSA ISSO and AAMVA's IT Security Officer will develop an action plan that promotes safeguarding CDL data as part of the CDLIS Modernization communication plan. The Agency anticipates completing the action plan by the end of calendar year 2009. Information developed as a result of the plan will be posted on FMCSA and AAMVA web sites. The Agency will also share with the States the importance of safeguarding CDL information as part of the CDL IT Users Workshop, scheduled for September 2009, and the CDL Coordinators Meeting, tentatively scheduled for February 2010.*

RECOMMENDATION 7: Prepare, in conjunction with the FMCSA CIO, contingency plans for CDLIS-Access, in accordance with OMB and NIST guidance.

RESPONSE: *Concur. Once CDLIS-Access is fully accredited, FMCSA will incorporate the system into its FISMA-compliant Information System Continuous Monitoring Program. The program, which operates in accordance with OMB and NIST guidance, includes continuity of operations, disaster recovery, and contingency planning. As part of the program, a contingency plan will be developed in accordance with scheduled security reporting, as documented in the Plan of Action and Milestones (POA&M). The POA&M will identify the tasks that must be accomplished, the resources required to perform these tasks, the milestones needed to achieve these tasks, and the scheduled completion dates for the milestones. FMCSA will ensure a contingency plan is prepared for CDLIS-Access in accordance with the POA&M and anticipates completing the plan, contingent on resources and agency priorities, by the end of FY 2010.*

RECOMMENDATION 8: Perform, in conjunction with the FMCSA CIO, disaster recovery testing of the CDLIS-Access system.

RESPONSE: *Concur. Once CDLIS-Access is fully accredited, FMCSA will work with the CDLIS-Access contractor and AAMVA to ensure that viable disaster recovery plans are maintained and, if necessary, updated in order to support the mission objectives during an unforeseen outage. This includes reviewing contingency plans and participating in scheduled disaster recovery contingency plan test exercises. Accordingly, FMCSA will perform disaster recovery testing of the CDLIS-Access system, contingent on resources and agency priorities, by the end of FY 2010.*

RECOMMENDATION 9: Promote and communicate to DMVs the need to perform periodic contingency testing for their licensing systems.

RESPONSE: *Concur. The FMCSA ISSO and the CDL Division will develop guidance for contingency testing of State licensing systems as part of the CDLIS Modernization communication plan. The guidance will inform States of best practices, and will be presented at*

Appendix A: Management Response

such forums as the CDL IT Users Workshop scheduled for September 2009 and the CDL Coordinators Meeting, tentatively scheduled for February 2010. Written documentation associated with this guidance and industry best practices for contingency planning and testing will be made available on the FMCSA and AAMVA web sites.

The FMCSA appreciates the OIG's efforts which assist FMCSA in fulfilling its transportation safety goals. If you need additional information or clarification, please do not hesitate to contact me, or Jeffrey K. Miller, Chief, Strategic Planning and Program Evaluation Division, 202-366-1258.