THOMAS A. SCHWEICH
Missouri State Auditor

September 9, 2013

Members of the General Assembly
and
John R. Mollenkamp, Acting Director
Department of Revenue
Jefferson City, Missouri

This letter relates to our review of the Department of Revenue's (DOR) drivers' license (DL) application process, the impact of the Federal Real ID Act - Title II Improved Security for Drivers' Licenses and Personal Identification Cards - of 2005 (the Act), and the sharing of the concealed carry endorsement data with other entities. Members of the Missouri Senate requested we review these matters in April 2013. The objectives of our review were to:

1. Evaluate procedures related to personal documents and data collected during the (DL) and non-drivers' license (ID) application and renewal process.

2. Evaluate compliance with rulemaking procedures relating to the scanning of certain documents during this process.

3. Evaluate compliance with Section 302.183[1], RSMo, which requires the privacy rights of applicants not be violated and prohibits the department from amending procedures for applying for a DL or ID to comply with the goals or standards of the Act.

4. Evaluate compliance with laws related to sharing of information related to holders of concealed carry endorsements with other entities.

5. Determine the impact to the state and its residents of failing to comply with the Act.

Our review determined the DOR did not consider certain risks to data collected during the DL application process, and violated state law by failing to promulgate a rule before requiring contract license offices to begin scanning certain DL and ID application documents (including Concealed Carry Certificates of Qualification). However, had the DOR promulgated a rule allowing scanning, the rule would have violated Section 302.183, RSMo. Either way a violation of state law occurred. In addition, the legislature should consider amending the law so that DOR can take actions to make DLs and IDs more secure while also protecting the personal information of private citizens. Finally, Missouri State Highway Patrol (MSHP) actions to share concealed carry endorsement license data complied with state law; however, the DOR and the OA-ITSD lacked a written agreement authorizing the OA-ITSD to provide this information to other entities.

[1] House Bill No. 361, First Regular Session, 95th General Assembly (2009)

Methodology

Our methodology included reviewing written policies and procedures, contracts, and other pertinent documents, and interviewing various personnel of the DOR and the MSHP, as well as certain external parties. We visited a DOR contract license office and observed processes in place regarding the scanning of documents. We also obtained an understanding of legal provisions that are significant within the context of the audit objectives, including applicable state and federal laws and regulations. In addition, we reviewed compliance with applicable federal grant agreements.

Background

Pursuant to Section 136.030(2), RSMo, the DOR has the authority and responsibility for the collection of motor vehicle registration fees, driver's license fees, motor vehicle sales and use tax, and all other taxes. Pursuant to Section 136.055, RSMo, the director of the DOR has competitively awarded contracts to 182 agents to operate contract license offices. The DOR, License Office Bureau, under management of the Motor Vehicle and Driver Licensing (MVDL) Division, is responsible for overseeing the contract license offices tasked with performing these functions. The DOR has contracted for DL computer hardware and support services with the same contractor[2] since 1972. Prior to awarding a new contract in 2010, the DOR issued DLs using an over the counter (OTC) system in which applicants received their licenses on the day of application. This procedure had been in place since 1995. However, due to aging equipment, the DOR performed a cost analysis of upgrading the system and identified three options with the following estimated annual cost:

- Third party central issuance - $3,680,000
- Continue over the counter issuance with new equipment - $5,116,500
- Internal central issuance administered by the DOR - $7,879,000

Based on cost estimates, and an expectation of increased DL data security, the DOR awarded the third party central issuance contract by competitive bid in October 2010. To offset some of the costs of the new system, the DOR applied for and received federal grants from the Department of Homeland Security in state fiscal years 2008 through 2011. The contractor provides license offices with computer equipment and the Office of Administration, Information Technology Services Division (OA-ITSD) provides the software system needed to process DL applications. The contractor also provided equipment to scan documents associated with DL applications. In accordance with contractual provisions of the previous and current contracts, equipment removed from the licenses offices is returned to the contractor when new equipment is installed. In addition, the DOR evaluated security procedures in place and added security features to provide additional safeguards against fraudulently issued DLs and IDs. In December 2012, the DOR instructed contract license offices to begin scanning DL application documents (including Concealed Carry Certificates of Qualification) and the contractor began issuing licenses to citizens under the new third party central issuance method.

Prior to December 2012, contract license offices photocopied certain application documents (such as documents of applicants asking for a review of their denied DL applications, as well as foreign passports,) and sent the documents to the DOR central office. The DOR scanned the photocopied documents and retained the images in a DOR database maintained by OA-ITSD. After December 2012, the images scanned by contract license offices were also retained in the database.

[2] The current contract is with Morpho Trust USA, Inc., which was created in 2011 when Safran acquired the division of L-1 Secure Credentialing, Inc. that held the DL contact. Various other predecessor firms held the contract prior to that time.

The Act modified U.S. law pertaining to security, authentication, and issuance procedures standards for state DLs and IDs. The law set requirements for IDs to be accepted by the federal government for official purposes determined by the Secretary of Homeland Security for the boarding of commercially operated airline flights and entering federal buildings and nuclear power plants. Several states expressed concerns related to privacy of applicant information. While the Act is optional for states, citizens of states that do not opt-in may not be able to use their state-issued DLs and IDs for official federal government purposes. According to the American Association of Motor Vehicle Administrators, as of February 25, 2013, there were 19 states complying with the Act, including the neighboring states of Iowa, Kansas, Nebraska, and Tennessee; while 16 states, including Missouri and Oklahoma, have laws prohibiting compliance with the Act. Requirements of the Act include retaining the application and source documents used to process state-issued DLs and IDs.

Under Section 32.091.7, RSMo, the DOR is not permitted to collect from DL applicants any information by which such persons can be individually identified, unless the department has specific statutory authorization to collect such information. Section 302.171.1, RSMo, requires the DOR to verify that applicants are a national of the United States or a noncitizen with a lawful immigration status, and a Missouri resident. This statute also allows the DOR to establish procedures to perform these verifications. Section 302.183.3, RSMo, states the DOR shall not amend procedures for applying for a DL or ID to comply with the goals or standards of the Act, any rules or regulations promulgated under the authority granted in such Act, or any requirements adopted by the American Association of Motor Vehicle Administrators for furtherance of the Act. On March 4, 2013, a Stoddard County resident filed a lawsuit against a license office contract agent and the DOR, alleging he was illegally denied a concealed carry endorsement on his DL for not allowing the license office to scan the Concealed Carry Certificate of Qualification obtained from the County Sheriff's office. On April 16, 2013, the Governor issued an order ending the scanning of all Concealed Carry Certificates of Qualification in contract license offices. Subsequently, the Legislature passed, and the Governor signed into law effective July 1, 2013, Senate Bill 252 that prohibits retention of source documents, with the following exceptions:

- Original application forms, which may be retained but not scanned
- Test score documents issued by state highway patrol driver examiners
- Documents demonstrating lawful presence of any applicant who is not a citizen of the United States, including documents demonstrating duration of the person's lawful presence in the United States
- Any document required to be retained under federal motor carrier regulations relating to the issuance of a commercial DL
- Any other document the applicant requests be retained by the DOR

On September 4, 2013, the Stoddard County Lawsuit was voluntarily dismissed.

Senate Bill 252 also requires the DOR to destroy, by December 31, 2013, all other DL applicant source documents obtained after September 1, 2012. In addition, the law specifically prohibits the DOR from retaining certificates of qualification for concealed carry endorsement. On July 1, 2013, the DOR instructed the license offices to only scan driver examination test papers, non-citizen documents demonstrating lawful presence, and commercial DL medical certifications. The DOR also contacted the Federal Motor Carrier Safety Administration to confirm that commercial DL medical certifications are the only documents the state needs to retain to comply with federal commercial DL requirements. As of August 2013, the federal agency has not contacted the DOR.

In November 2011 an investigator with the Social Security Administration (SSA), Office of the Inspector General, requested a list of state concealed carry endorsement holders from the MSHP. Pursuant to the memorandum of agreement between the MSHP and the DOR for sharing of DL and ID information for

investigative purposes, the MSHP forwarded the request to the OA-ITSD unit that maintains the DOR systems.

The OA-ITSD generated the list of state concealed carry endorsement holders and sent a compact disc to the MSHP, which then mailed the disc to the SSA Investigator. The data fields on the compact disc included the name, social security number, date of birth, and gender of each concealed carry endorsement holder. However, according to testimony by the SSA investigator to the Senate Appropriations committee, the investigator was not able to read the data provided and destroyed the disc. In January 2013, the SSA investigator again requested this data and a disc was generated and sent in the same manner as the initial disc. However according to legislative committee testimony, the SSA investigator again was unable to access the information and destroyed the disc. In February 2013, the OA-ITSD placed the list on a secure password protected File Transfer Protocol website and sent the password to the SSA investigator. The OA-ITSD stated the website was accessed five times the day the link was sent; however, the SSA investigator contacted the MSHP and stated he was unable to view the data and requested a third disc be provided. The OA-ITSD provided the MSHP a third disc in February 2013 but the SSA investigator did not retrieve it. As a result, the MSHP sent the disc back to the OA-ITSD in March 2013. According to the OA-ITSD, it automatically disables secure websites after 30 days and deletes all data.

During a legislative committee hearing, the SSA investigator provided an email message showing the website and password provided to him to access the concealed carry endorsement holder list. Subsequently, a computer registered to the House of Representatives (House) attempted to access the secure website using the password in the email message. The OA asked the House for the records documenting which computer was used and the person who attempted to access the secure site. The House denied the request and has not released the requested information. This matter could potentially be addressed by authorities and will not be addressed further in this letter.

The Legislature reduced DOR appropriations funding the contract for issuing DLs and IDs, and boat and ATV registrations, essentially funding these activities for only 8 months of state fiscal year 2014. The Legislature has indicated it will reconsider the DOR budget during the next legislative session beginning in January 2014, contingent upon the DOR discontinuing the practice of scanning documents related to applications for DLs and IDs.

In May 2013, the House of Representatives created the Bipartisan Investigative Committee on Privacy Protection to review the state's handling of personal identifying information related to the application for state-issued DLs and IDs and concealed carry endorsements on DLs and IDs. This Committee includes legislators and non-legislators. In July 2013, due to questions of whether or not a committee including non-legislators had subpoena power, the Special Interim Committee on Privacy Protection, made up entirely of legislators, was created so the Bipartisan Investigative Committee on Privacy Protection could obtain information via subpoena.

Results, Conclusions, and Recommendations

1. Safeguards to Protect Personal Information

While the DOR implemented safeguards to protect the personal information collected, it did not fully consider risks related to the personal data collected and scanned by contract license office personnel. In addition, our review of data feeds sent to the DOR contractor observed no scanned documents.

Contract license office personnel scanned birth certificates, items proving applicant address such as bank statements or photocopies of utilities bills, and documents related to DL endorsements including Concealed Carry Certificates of Qualification. Certain documents including passports that are too thick to

be scanned and crumpled documents, which could include birth certificates, cannot be scanned without first being photocopied. DOR personnel indicated they did not consider the potential risks of networked photocopiers, internal hard drives in the photocopiers, or fax machines attached to photocopiers as a possible ID theft target. As a result, contract office employees could obtain personal data by emailing or faxing the scanned documents to a personal account, or by accessing the internal memory of photocopy machines.

The OA-ITSD has various security procedures in place to protect the data on ITSD servers. These procedures include security patch management, internet filtering, spam detection, network access control, State Data Center physical security, authentication and authorization, and intrusion prevention systems. Access to perform these procedures require specific employee credentials that can include usernames, passwords, and biometric information, such as fingerprints. While it appears OA-ITSD has made an effort to secure the information obtained, no system or data center can be completely secure. The scanning of applicant information that includes personal bank statements results in information needed for identity theft to be compiled in a single database. Similar concerns were raised in comments on the REAL ID Final Rule (Federal Register, Volume 73 Issue 19). One comment referred to this compilation of information as an "identity thief's dream target."

We recommend the DOR consider the identity theft concerns related to personal data and immediately develop policies and procedures to mitigate these risks.

2. Compliance With Rulemaking Procedures

The DOR's failure to promulgate a state rule violates the holding of Young v. Children's Division, State Department of Social Services, 284 S.W.3d 553 (Mo. Banc 2009), because no statute or rule notifies the public that they must allow the DOR to photocopy and/or scan their birth certificates to obtain a DL or ID.

While the DOR has the authority under state law to require individuals seeking a DL or ID to verify residency and to show photocopies of birth certificates, state law did not address whether the DOR may photocopy or scan these documents. In addition, according to Section 32.091.7, RSMo, the DOR is not permitted to collect from DL applicants any information by which such persons can be individually identified, unless the department has specific statutory authorization to collect such information. In April 2013, after legislators raised issues related to the lack of a state rule, the DOR submitted preliminary information to the Joint Committee on Administrative Rules to begin the rule making process.

We recommend the DOR comply with the rule making requirements in the future.

3. Real ID Compliance

The DOR implemented additional provisions of the Act after the state law prohibiting compliance became effective in 2009. In addition, the DOR had complied, or had planned to comply, with most substantial provisions of the Act. However, because the DOR violated state law by failing to promulgate a rule (as described in Finding No. 2 above), DOR actions to scan DL application documents (including Concealed Carry Certificates of Qualification) did not technically violate the state law prohibiting compliance with the Act. However, the legislature needs to review state law as it could be interpreted so that DOR cannot make DLs and IDs more secure.

Section 302.183, RSMo, prohibits the DOR from amending procedures for applying for a DL or ID to comply with the goals and standards of the Act. According to DOR personnel, prior to the 2009 adoption of this statute section, the state had already complied with 20 of the 39 Act requirements and had partially implemented 15 provisions. Three years later, in December 2012, the DOR submitted a letter to the U.S. Department of Homeland Security (DHS) stating the DOR had met 22 of 39 Act requirements. The letter

also indicated the DOR planned to fully or partially comply with 13 more requirements, including 5 additional requirements in 2013 (2 of these provisions were required under federal commercial DL laws). The DOR did not intend to comply with the remaining 4 requirements of the Act which include 1) placing an indicator on the DL or ID stating the state is compliant with the Act, 2) committing to be in full compliance with the Act by January 1, 2010, 3) clearly stating on the face of non-compliant DLs or IDs that the card is not acceptable for official purposes, and 4) submitting a final certification package to the DHS, which includes a statement from the Governor certifying the state is in compliance with the Act and a letter from the Attorney General confirming the state has the legal authority to impose the Act requirements. The DOR also did not intend to fully comply with provisions of seven other Act requirements, including verifying applicants' social security numbers with the SSA and verifying applicants' birth certificates in the Electronic Verification of Vital Events database. In addition, the DOR can no longer comply with the requirement of the Act that requires retention of applications, declarations, and source documents due to restrictions contained in Senate Bill 252.

A federal commission proposed standardizing state-issued identifications after noting most terrorists involved in the 9/11 attacks used false identification to board airplanes. DOR personnel indicated they implemented various requirements not to comply with the goals or standards of the Act, but to make DLs and IDs more secure. DOR personnel also stated that because the Act basically consisted of a compilation of best practices used in various states to enhance security, there is an overlap between the Act and current DOR DL and ID procedures, and it is the DOR's responsibility to provide secure DLs and IDs to prevent fraudulent reproduction. However, considering the DOR is compliant with most of the Act's requirements, and the obvious goal of the Act is to make DLs and IDs more secure, it raises questions as to whether the DOR is in compliance with state law. From a technical standpoint, the DOR would have had to promulgate a rule regarding the scanning of documents to be in violation of Section 302.183, RSMo, since this statute states the DOR cannot "amend procedures" for applying for a DL or IDs in order to comply with the goals or standards of the Act. Therefore, because the DOR violated state law by not formally amending its procedures through the rulemaking process (see Finding No. 2 above), changes the DOR put in place to scan DL and ID application documents (including Concealed Carry Certificates of Qualification) were not enforceable, and therefore did not violate Section 302.183, RSMo. If the DOR had followed state law regarding the rulemaking process by promulgating a state rule related to the new DL and ID processes, its actions to formally amend DL and ID processes would have violated Section 302.183, RSMo. Either way the DOR violated state law.

The current state law prohibits the DOR from amending procedures to comply with the goals of the Act, with the main goal being improved security for DLs and IDs. However, it is unlikely the legislature intended to prevent the DOR from implementing certain changes to make DLs and IDs more secure. As a result, it appears prudent that the legislature should enact necessary changes to protect the information of private citizens without prohibiting the DOR from improving security for DLs and IDs.

We recommend the legislature consider amending state law so private personal information is protected while not making it illegal for the DOR to make DLs and IDs more secure.

4. Written Agreement Between DOR and OA-ITSD

The OA-ITSD did not contact the DOR for permission, and no written agreement was in place authorizing the OA-ITSD, to provide DOR DL data (including concealed carry enforcement data) to the MSHP.

The DOR informally agreed to allow the OA-ITSD to provide investigative information to the MSHP without prior approval from the DOR. This informal agreement consisted of email messages between the DOR and the OA indicating law enforcement agencies could contact OA-ITSD directly with specific requests for DL data. As previously discussed in our report No. 2011-56, *Revenue, Taxation Division*

Security Controls, the DOR's and the OA-ITSD's memorandum of understanding related to the services provided to the DOR by the OA-ITSD, has not been updated since 2006 and lacks critical information, such as defining operational and security responsibilities for each organization, and therefore does not address MSHP requests for DL data. DOR personnel stated they drafted an updated agreement in November 2011, however, the DOR and OA-ITSD never finalized the agreement.

While it appears the OA-ITSD's sharing of DL data with the MSHP was not a violation of law, a formal agreement is necessary to ensure the current and future security of DOR data maintained by the OA-ITSD.

We recommend the DOR enter into a written agreement with the OA-ITSD formalizing the OA-ITSD's authority for sharing DL data.

Matters Not Requiring Corrective Action

Scanned Documents

Legislative concerns included the possibility that scanned documents were sent to the DL contractor that maintains relationships with various governmental entities, including the federal government. However, we viewed data feeds traveling from the DOR to the contractor and observed no scanned documents being sent.

Sharing of Concealed Carry Endorsement List

MSHP actions to share the concealed carry endorsement list with the SSA investigator appear to be authorized under state law. Section 43.659, RSMo, allows the MSHP to enter into a memorandum of understanding with other governmental agencies including the federal government. While Section 571.101.9, RSMo, makes concealed carry holder information a closed record, Section 610.120, RSMo, states that closed records may be accessible to federal agencies for investigative purposes, and Missouri Attorney General's Opinion No.106, 1996 to McManaman, referred to case law which held that closed records are available to law enforcement and federal agencies for investigative purposes regardless of a statutory provision closing these records. According to Title 5, Section 6 of the Inspector General Act, the Office of the Inspector General is authorized as a law enforcement agency. Based on this information, the MSHP provided the information to a law enforcement agency as legally permitted.

DHS DL Security Grants

During state fiscal years 2008 through 2011, the DHS awarded the DOR approximately $3.2 million in DL security grants. The 2008 grant, entitled "Real ID Demonstration Grant Program", included requirements for the state to meet 15 specific benchmarks related to the Act. In subsequent years, the DHS renamed the grant "Driver's License Security Grant Program" and dropped requirements of the Act. It is not clear why the DHS changed the grant name and dropped "REAL ID" terminology. However, DHS actions to change the grant name and remove all mention of the Act could be interpreted as an attempt to encourage the 16 states with laws prohibiting implementation to comply with the Act.

Impact of not Complying with the Federal Real ID Act of 2005

At this time, the full ramifications for citizens of states choosing not to comply with the Act are not clear. According to the Act's Final Rule (Federal Register, Volume 73, Issue 19), beginning May 11, 2008, federal agencies were to refuse access (including boarding federally-regulated commercial aircraft, accessing federal buildings that require identification, and entering nuclear power plants) to individuals with DLs or IDs not complying with the Act, unless the issuing state had requested and obtained an extension of the compliance date from DHS. The DHS has extended this deadline several times, with the DHS most recently granting a deferment of at least 6 months past the January 15, 2013 deadline. According to the DHS, individuals will still be able to board aircraft with a DL or ID issued by states not

meeting the requirements of the Act; however, these individuals will have to follow the procedures of someone without a DL or ID and will require additional screening before boarding. It is not clear what these additional screening procedures entail. It is also not clear when the DHS will begin enforcing these non-compliant DLs and IDs procedures.

Sincerely,

Thomas A. Schweich
State Auditor

CC: Honorable Jeremiah W. (Jay) Nixon, Governor

Colonel Ronald K. Replogle, Superintendent
Missouri State Highway Patrol

Douglas Nelson, Commissioner
Office of Administration