DEPARTMENT OF PUBLIC SAFETY
Driver License Division

Information Systems Audit of the
Driver License Database
December 21, 2018

Report No. IT 18-03

OFFICE OF THE
STATE AUDITOR

AUDIT LEADERSHIP:
John Dougall, State Auditor
Ethan Heintzelman, CPA, CISA, Director

DEPARTMENT OF PUBLIC SAFETY

Driver License Division

December 21, 2018

TABLE OF CONTENTS

Background

Uniform Driver License Act

In 1993, the Utah Legislature passed and the Governor signed S.B. 19, Department of Public Safety (DPS) Reorganization, which officially designated the Uniform Driver License Act (UDLA) and statutorily created the Driver License Division (DLD).[1] The duties assigned in statute to DLD include the duty to "[establish] procedures for the storage and maintenance of [driver license] applicant information."[2] Applicant information may include the applicant's full legal name, birth date, gender, fingerprints, photograph, and proof of valid Social Security Number (SSN). This information is currently stored and maintained in an electronic driver license database (Database). The Department of Technology Services (DTS) assists DLD in operating and maintaining the database.[3]

Access to the Driver License Database

Database user accounts are provided to DPS employees based upon their job title and responsibilities.

[1] Laws of Utah, 1995 General Session, Ch. 333.
[2] Utah Code § 58-37f-201(2).
[3] Utah Code § 58-37f-201(3).

Audit Objectives, Scope, Methodology, and Limitations

The audit was conducted to assess the quality of security and access controls for the Driver License Division's (DLD) database of applicant information (Database). Our audit scope included a review of the following data and documentation for fiscal year 2018:

- Applicable state statutes and administrative rules.
- Applicable DTS, DPS, and DLD policies and procedures.
- Audits and risk assessments conducted by DTS, DPS, the Federal Bureau of Investigations, and the Office of the Legislative Auditor General.
- Evidence of configured password policies for applications, databases, servers, and networks relevant to Database operations.
- User and administrator listings for applications, databases, servers, and networks relevant to Database operations.
- Logs of Database user activities.
- DTS change tickets documenting and authorizing changes to applications, databases, servers, and networks relevant to Database operations.
- Logs of changes to the Database and its associated code repository.
- Documentation of backup schedules and restoration testing for applications, databases, and servers relevant to Database operations.
- DPS record of employee histories.

In addition to our review of applicable documentation, we conducted interviews with process owners and stakeholders to understand Database operations and relevant IT controls. Using the information provided in these interviews combined with our review of relevant evidence, we documented the design of approximately 20 IT controls related to the following areas: logical access, computer operations, change management, and data security.

Having documented the design of our selected IT controls, we conducted a series of tests to verify that each control operated according to its intended design. Where feasible, if a control did not operate as intended or we deemed it was not designed effectively, we looked for any substantive findings associated with the failed control.

Findings

Finding 1: Password requirements for Database administrators do not conform to required DTS policy

Control Category	Logical Access: Database and Server Passwords
Condition	Password requirements for back-end Database administrators do not comply with the official DTS policy adopted by DPS. The following table summarizes deficiencies in the existing implementation:
Effect	Increased susceptibility to unauthorized access to Database and system infrastructure.
Recommendations	1. DLD should comply with DPS policy by enforcing the DTS enterprise-wide password requirements on all database and server accounts. 2. DLD should require multi-factor authentication to access sensitive systems or data.

DTS Policy	Database	Servers (4 servers tested)
Password should be 8+ characters	No requirement enforced	1 server permitted passwords of 5+ characters
Passwords must include at least 3 character types (uppercase, lowercase, numeric, special)	No requirement enforced	No requirement enforced
Passwords must be changed at least every 90 days	No requirement enforced	3 servers had no requirement
A user's 10 most recent passwords may not be reused	No requirement enforced	3 servers prevented reuse of only the single most recent password
A user will be disabled after 3 unsuccessful password attempts	User disabled after 10 unsuccessful password attempts	No disabling of users after unsuccessful password attempts

Entity's Response:

We will enforce a password policy for database administrator connections to the driver license database: passwords should be 8+ characters, passwords must include at least 3 character types, passwords must be changed at least every 90 days, a user's 10 most recent passwords may not be reused, a user will be disabled after 3 unsuccessful password attempts.

Finding 2: Several individuals retained Database user accounts after being terminated from DPS employment

Control Category	Logical Access: Authorized Users
Condition	Database user accounts are provided to DPS employees based upon their job title and responsibilities. Hiring practices, including interviews and background checks, help ensure that only qualified individuals receive access to the database. However, procedures to ensure that Database user accounts are de-provisioned when individuals are no longer authorized (e.g., employment is terminated) appear to be inadequate. A review of 108 terminated DPS employees from fiscal year 2018 showed 8% retained Database user accounts after termination. Mitigating controls are in place to prevent unauthorized access in such cases (e.g., the terminated employee must first authenticate to the State network). However, the existence of active Database user accounts for terminated employees increases the risk that confidential information may be accessed inappropriately.
Effect	Unnecessary risk of unauthorized access to PII in the driver license database
Recommendation	DLD should implement procedures and controls to ensure that Database user accounts for all terminated employees are revoked in a timely manner following their termination.

Entity's Response:

Driver License does have a termination policy that outlines that the Driver License Help Desk should be notified when an employee is terminated. The termination policy will be followed to comply with the audit finding.

Finding 3: Database user accounts are not periodically reviewed for appropriateness

Control Category	Logical Access: Authorized Users
Condition	DLD does not perform regular reviews of Database user accounts for appropriateness. DLD does not conduct regular reviews of system administrators at the database, server, or network levels. Periodically performing these reviews would enable DLD to identify inappropriate user accounts associated with terminated employees, as well as accounts with permissions no longer required by the associated user.
Effect	Unauthorized users may retain access to the Database servers, database, and/or application subsequent to an action (e.g. termination, transfer, retirement, etc.) that would render their access unlawful.
Recommendation	DLD should carry out periodic access reviews on all Database-related systems, revising access controls as appropriate.

Entity's Response:

We will implement a bi-annual review of IT personnel with access to the Driver License database at the network, database, and server levels.

Finding 4: Insufficient monitoring of testing documentation for application changes prior to deployment

Control Category	Change Management: Control of Changes Migrating from Testing to Final Approval
Condition	DLD contracts with DTS to administer the Database application change management process. DTS tracks and controls changes via change tickets and version control software. DLD's application development procedure requires an independent member of the Acceptance Testing (AT) team to test each developer change before deploying the change to production. However, existing controls provide insufficient assurance that developers adhere to this procedure. In particular, DLD's ticketing system does not prevent project managers from approving deployment to production before a change has been tested by the AT team. Furthermore, project managers do not verify that independent testing has been performed before giving approval for deployment to production. Forty percent of application changes we sampled lacked evidence of independent testing before deployment to production.
Effect	Code that has not been appropriately tested could be implemented in the Database.
Recommendation	DLD should implement procedures to ensure that all modified code has been independently tested prior to deployment to a production environment.

Entity's Response:

The Driver License Quality Assurance team is highly involved in deployments to production. In some cases, deployments have been done without an official paper-trail through the Redmine ticketing system. Going forward, we will take steps to ensure that this part of the process is not overlooked.

State of Utah

GARY R. HERBERT
Governor

SPENCER J. COX
Lieutenant Governor

Department of Public Safety

JESS L. ANDERSON
Commissioner

September 4, 2019

John Dougall
Office of the State Auditor
East Office Building, Suite E310
Utah State Capitol Complex
Salt Lake City, Utah 84114

Dear Auditor Dougall:

I am writing to provide an update on progress made toward addressing the findings identified in the Information Systems Audit of the Driver License Database Report (No. IT 18-03), which was dated December 21, 2018. Following the release of the report, the Department of Public Safety and its Driver License Division (DLD) immediately developed a plan of action to address each of the four findings. A brief response to the findings was provided for insertion into the audit report before it was finalized. Below is an update and additional information on how the Department worked to ensure the findings were addressed and to correct the issued identified in the report.

Finding 1 Response: DLD follows a password policy for database administrator connections to the driver license database: passwords should be 8+ characters, passwords must include at least 3 character types, passwords must be changed at least every 90 days, a user's 10 most recent passwords may not be reused, a user will be disabled after 3 unsuccessful password attempts. Database administrators were adhering to the state's policy but it was determined that the system was not validating that the standards were being met and enforced among all users. An update to the system was made immediately to ensure that password standards were being enforced by the systems.

Finding 2 Response: DLD has a termination policy that outlines that the Driver License Help Desk should be notified when an employee is terminated so they can be removed as a database user. The division has updated training and exit interview forms to ensure that supervisors disable an employee's access when they leave the division. Additional training has been provided to supervisors to remind them of the importance of disabling logins as part of an exit interview. The division has created an automated report that will show a list of users that have not logged into the DLD system for a period of time. This list will be examined periodically to determine if there are logins that need to be disabled.

Finding 3 Response:
Database user accounts were reviewed at the time of the release of the audit report. All access to accounts were found to be appropriate. DLD has instituted a periodic review of accounts. To support this effort, DTS has created a script that will automatically email the

DTS director with a list of individuals who have access to the database. This list will be reviewed and employees will be removed, when appropriate.

Finding 4 Response:
DLD has a thorough development, testing, acceptance, and deployment process for routine, everyday work. The audit took a snapshot during a window of time when the division was having difficulty integrating with a 3rd party system that did not have a robust test environment. A secondary review of this process should yield sufficient results leading to no findings. In addition, the Driver License Quality Assurance team is highly involved in deployments to production; yet, in some cases, deployments have been done without an official paper-trail through the electronic ticketing system. Going forward, DLD will take steps to ensure that this part of the process is not overlooked.

The Department is committed to ensuring quality security and access controls for any database administered by the agency or its divisions. We appreciate you and your team's efforts to identify issues that needed to be addressed and appreciate your support while the Department made corrections and improvements. If you have any questions regarding the information provided, please don't hesitate to contact me at 801-971-3294 or via email at krigby@utah.gov.

Kristy K. Rigby

Deputy Commissioner