

Law Enforcement's Use of State Databases

Update to 2013 Evaluation Report

Problems Identified

- **Inappropriate Viewing of Private Data.** Some law enforcement personnel used their access to driver's license data for non-work purposes or for work purposes not allowed by state law. Neither Driver and Vehicle Services (DVS) nor the Bureau of Criminal Apprehension (BCA) did much monitoring to identify misuse or had a written policy for sanctions when misuse by law enforcement personnel was discovered.
- **Inadequate Training and Data-Access Controls.** The Department of Public Safety (DPS) did not have adequate training policies for all law enforcement users of driver's license data, and controls over access to those data or the Comprehensive Incident-Based Reporting System (CIBRS) were not always effectively implemented.

Changes Implemented

- **Strengthened Controls Over Access to Driver's License Data.** BCA created a new application—DVS Access—for law enforcement personnel to access driver's license and motor vehicle data. Law enforcement users can access these data only through BCA's secure network and dedicated computers. Previously, users could view the data from any computer with Internet access. Law enforcement personnel accessing driver's license photos must indicate the purpose of the query.
- **Improved Policies and Training.** DPS worked with statewide associations representing sheriffs and police chiefs to develop a model policy that addresses use of driver's license data. In addition, BCA revised its policies that outline appropriate uses of data accessed through its systems. Law enforcement personnel must complete training and certification before accessing the new DVS Access application, with retraining and recertification every two years. BCA revised its training on appropriate uses of CIBRS data, too.
- **More Monitoring of Driver's License Data Use and Timelier CIBRS Audits.** DVS started conducting random audits of law enforcement agencies' use of driver's license data. In addition, BCA implemented an audit tool that analyzes patterns of data use to identify possible anomalies. Finally, BCA reports that CIBRS audits are up-to-date and audits of newly participating CIBRS agencies are completed within six months.

Action Needed

- **Continue to Develop BCA Audit Tool.** BCA and local law enforcement agencies need to develop business rules to enhance the ability of this tool to identify possible data misuse.
- **Limit Access to CIBRS.** BCA officials intend to centralize access to CIBRS for the purpose of providing access only to certified law enforcement personnel. This should be completed within two years, according to BCA.