OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

Evaluation Report Summary / February 2013

Law Enforcement's Use of State Databases

The state's approach to managing law enforcement's use of state databases is reasonable, but monitoring and accountability need to be strengthened.

Key Facts and Findings:

- During fiscal year 2012, over 11,000 law enforcement personnel accessed driver information of more than 1.4 million individuals through the Driver and Vehicle Services (DVS) Web site.
- The Legislature authorized Minnesota's Comprehensive Incident-Based Reporting System (CIBRS) in 2005 to facilitate information sharing among law enforcement agencies, but its use has been limited. In fiscal year 2012, only 62 users searched the database.
- Some law enforcement personnel have used their access to driver's license data for non-work purposes or work purposes that are not allowed by state law.
- The Department of Public Safety (DPS) has not had adequate training policies for all law enforcement users of driver's license data, and access controls have not always been effectively implemented.
- DVS and the Bureau of Criminal Apprehension (BCA) maintain records of law enforcement queries of driver's license data, but neither division does much monitoring of the records to identify misuse or has a written policy for sanctions when misuse is found.
- Law enforcement personnel have used CIBRS in ways that statutes do not permit.
- BCA's practices to limit access to CIBRS have not prevented some searches by law enforcement staff without proper certification, and its audit practices have not adequately detected and addressed violations of state law.

Key Recommendations:

- DPS and chief law enforcement officers need to increase awareness among law enforcement staff about the classification and allowed uses of driver's license data.
- DPS should strengthen controls over access to driver's license information, particularly access through the DVS Web site.
- DPS should consider increasing its resources for monitoring use of driver's license data, and chief law enforcement officers should consider doing a greater number of proactive audits of their employees' use.
- BCA should ensure that only certified users have access to CIBRS and should explicitly address in training the recurring misuses of CIBRS.
- BCA should improve implementation of its CIBRS audit program and use the system's audit trail to identify inappropriate use between audits.
- The Legislature should amend the CIBRS section of statutes so that some information about agencies that participate in CIBRS, such as their names, is public.

Room 140 Centennial Building, 658 Cedar Street, St. Paul, Minnesota 55155-1603 • Tel: 651-296-4708 • Fax: 651-296-4712
E-mail: auditor@state.mn.us • Web Site: www.auditor.leg.state.mn.us • Through Minnesota Relay: 1-800-627-3529 or 7-1-1

Law enforcement personnel's misuse of state databases has included non-work-related and work-related uses that are not permitted by law.

Report Summary

Law enforcement agencies use a wide variety of information to protect public safety and enforce the law. Some of the information they access is in state databases that contain a significant amount of personal data. The Department of Public Safety (DPS) provides law enforcement personnel with access to driver's license data and the Comprehensive Incident-Based Reporting System (CIBRS), among other databases.

The state driver's license database contains information, including photographs, for every person who has a Minnesota driver's license or identification card. The Driver and Vehicle Services Division (DVS) collects and maintains driver's license data. Law enforcement personnel access these data through a DVS Web site or through systems operated by the Bureau of Criminal Apprehension (BCA).

CIBRS is a database to which Minnesota law enforcement agencies voluntarily submit data about incidents that may be of interest to other Minnesota law enforcement agencies. For a given incident, CIBRS can contain information about the date, time, location, and type of offense, as well as information about any persons or property involved. BCA manages CIBRS.

Law enforcement personnel make extensive use of driver's license information, but less use of CIBRS.

During fiscal year 2012, law enforcement users performed about 3.8 million queries of driver's license information through the DVS Web site. They made even greater use of driver's license information through BCA systems. Between January and March 2012, law enforcement staff performed more than three times as many queries of driver's license information through BCA systems as through the DVS Web site.

Personnel from 29 law enforcement agencies performed 333 CIBRS searches in fiscal year 2012. As of July 2012, 150 of the state's roughly 435 law enforcement agencies had had access to CIBRS at some point since the first agency began participating in December 2006.[1]

Some law enforcement personnel have accessed driver's license data for impermissible purposes.

With some exceptions, federal and state laws classify personal driver's license data as private and limit their permissible uses.[2] The permissible law enforcement use is broad for most driver's license information, but uses of photographs are more limited.

We defined inappropriate use as accessing the driver's license database using invalid privileges or without a permissible purpose. It includes non-work-related use or work-related use that is not permitted by law. Use does not need to be malicious or for personal gain to be inappropriate.

DVS records of fiscal year 2012 investigations into possible misuse of its Web site showed that 88 law enforcement personnel misused DVS data. We also identified some misuse. For example, some users continued to access the Web site using usernames and passwords associated with their previous employment. In interviews, some law enforcement officials described work-related uses of driver's

[1] There were approximately 450 law enforcement agencies in Minnesota in 2012, but state statutes authorize only some law enforcement agencies to participate in CIBRS. *Minnesota Statutes* 2012, 299C.40, subd. 1(c).

[2] *18 U.S. Code* 2721-25 (2006); and *Minnesota Statutes* 2012, 171.07, subd. 1a; and 171.12, subds. 7(a) and 7a.

Reducing misuse of state databases by law enforcement staff will require efforts by the Department of Public Safety and law enforcement officials.

license photographs that are inconsistent with state law.

Other queries of driver's license information appeared questionable. For example, the DVS "audit trail," which records queries of driver's license information, showed that over half of the law enforcement users queried information of people with their same name or same surname, or disproportionately queried records of individuals of one sex or the other during fiscal year 2012.

DPS and law enforcement officials need to strengthen training and access controls for driver's license data and consider increasing resources to monitor their use.

Chief law enforcement officers should consider requiring all of their employees who use driver's license data to take DVS's training. Currently, sworn officers who use the Web site are not required to do so. Law enforcement personnel who access driver's license information through BCA systems must take training, but it does not specifically cover proper use of driver's license information. The DVS training released in January 2013 covers classification and permissible uses of driver's license data, including photographs, and possible consequences for misuse.

DPS should also work with the Sheriffs' Association and Chiefs of Police Association to develop a model policy on law enforcement use of driver's license data.

DVS needs to strengthen access controls. Authorized users can access its Web site from any computer with Internet access, so it is important that only persons who need access have it, and that they have access to only the information they need. DVS should obtain user agreements from law enforcement agencies that use the Web site, work with agencies to make sure user accounts are disabled when no longer needed, and work toward granting access to historical driver's license photographs more selectively.

Currently, chief law enforcement officers provide the best opportunity for effective proactive monitoring of their employees' data use. They are in the position to know employees' work schedules and responsibilities and thus have a greater chance of recognizing uses inconsistent with those required by their job. We recommend that law enforcement agency leaders consider doing more proactive monitoring.

Finally, DPS should consider (1) increasing its resources—personnel and technology—for monitoring use of driver's license information and (2) formalizing its approach to handling inquiries about use of this information.

Some law enforcement personnel have searched CIBRS for work purposes that are not among those allowed by law.

State statutes classify CIBRS data as not public and limit their use to six purposes.[3] However, some personnel have used CIBRS for other work-related purposes, such as gun permit checks and some employment background checks. CIBRS can be used for employment background checks only for sworn officers or positions that could lead to employment as a sworn officer.

BCA needs to increase the information it provides about appropriate uses of CIBRS, ensure that only certified users have access to the system, and improve the CIBRS audit program.

BCA requires training of CIBRS users that covers appropriate use of the system, but some users still access CIBRS for inappropriate purposes.

[3] *Minnesota Statutes* 2012, 299C.40, subds. 2 and 4.

Laws and policies that regulate law enforcement's use of state databases must balance needs and interests that often conflict.

BCA should include in its training not only authorized uses, but also explicit discussion about the inappropriate uses that have been found. BCA should also monitor the CIBRS audit trail between regularly scheduled audits to identify and halt misuse, and should periodically remind CIBRS users about the permissible uses of the system.

BCA needs to better control access to CIBRS. State statutes require that only certified users have access to the system.[4] BCA implements this by requiring each law enforcement agency to ensure its users are trained and tested. Law enforcement agencies have not always accurately recorded users' test information, though. As a consequence, users who have not completed certification have had access to CIBRS.

Finally, BCA needs to improve the CIBRS audit program. Although BCA has a goal of auditing all CIBRS agencies within their first six months, it has missed this goal numerous times. Several agencies have never been audited. In addition, auditors' reviews of CIBRS searches do not always require complete justifications for the searches. State law limits CIBRS uses, and it is important that compliance with these limited uses be monitored.

Creating policy surrounding law enforcement's use of state databases involves the difficult task of balancing public safety needs with civil liberties, privacy, and transparency interests.

Law enforcement agencies need to collect, create, and share information to protect public safety. At the same time, law enforcement's use of personal data raises civil liberties, privacy, and transparency concerns.

To balance these sometimes conflicting needs and interests, the Legislature, DPS, and law enforcement agencies use various tools, including data collection and retention rules, data classification, and access and use restrictions. Training and audits, two additional tools, provide ways to inform users about classifications, rules, and restrictions, and monitor users' compliance with them.

The Legislature and DPS have used many of these mechanisms for driver's license data and CIBRS. Overall, we think the approaches the state has taken are reasonable. But as implemented, the mechanisms do not adequately address privacy and transparency concerns about law enforcement's use of driver's license data. The classification of CIBRS data limits transparency about the system. In addition, the cumulative effect of mechanisms to address privacy, transparency, and civil liberties interests may be limiting CIBRS' potential to meet public safety and information-sharing needs.

[4] *Minnesota Statutes* 2012, 299C.40, subd. 5.

Summary of Agency Response

In a letter dated February 5, 2013, Department of Public Safety (DPS) Commissioner Ramona Dohman said sensitive data must be available to law enforcement officers for them to carry out their public safety responsibilities and solve crime. She said DPS strongly agrees that these data "should not be accessed in a manner that violates the trust the citizens of our state have a right to expect." The commissioner said DPS commits to strengthening oversight and user training, and she listed several efforts already underway. She noted, however, that "no amount of oversight or training is a substitute for an individual honoring his or her professional and ethical obligation as an officer of the law," and said DPS "will continue to stress to all users the importance of accessing this data in a legal and ethical manner."

The full evaluation report, *Law Enforcement's Use of State Databases*, is available at 651-296-4708 or:
www.auditor.leg.state.mn.us/ped/2013/ledatabase.htm