OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

EVALUATION REPORT

Law Enforcement's Use of State Databases

FEBRUARY 2013

PROGRAM EVALUATION DIVISION
Centennial Building – Suite 140
658 Cedar Street – St. Paul, MN 55155
Telephone: 651-296-4708 • Fax: 651-296-4712
E-mail: auditor@state.mn.us • Web Site: http://www.auditor.leg.state.mn.us
Through Minnesota Relay: 1-800-627-3529 or 7-1-1

Program Evaluation Division

The Program Evaluation Division was created within the Office of the Legislative Auditor (OLA) in 1975. The division's mission, as set forth in law, is to determine the degree to which state agencies and programs are accomplishing their goals and objectives and utilizing resources efficiently.

Topics for evaluations are approved by the Legislative Audit Commission (LAC), which has equal representation from the House and Senate and the two major political parties. However, evaluations by the office are independently researched by the Legislative Auditor's professional staff, and reports are issued without prior review by the commission or any other legislators. Findings, conclusions, and recommendations do not necessarily reflect the views of the LAC or any of its members.

A list of recent evaluations is on the last page of this report. A more complete list is available at OLA's web site (www.auditor.leg.state.mn.us), as are copies of evaluation reports.

The Office of the Legislative Auditor also includes a Financial Audit Division, which annually conducts an audit of the state's financial statements, an audit of federal funds administered by the state, and approximately 40 audits of individual state agencies, boards, and commissions. The division also investigates allegations of improper actions by state officials and employees.

Evaluation Staff

James Nobles, *Legislative Auditor*

Joel Alter
Valerie Bombach
Sarah Delacueva
Jody Hauer
David Kirchner
Carrie Meyerhoff
Judy Randall
Jodi Munson Rodriguez
Matt Schroeder
KJ Starr
Julie Trupke-Bastidas
Jo Vos
Lang (Kate) Yang

To obtain a copy of this document in an accessible format (electronic ASCII text, Braille, large print, or audio), please call 651-296-4708. People with hearing or speech disabilities may call us through Minnesota Relay by dialing 7-1-1 or 1-800-627-3529.

All OLA reports are available at our Web site: http://www.auditor.leg.state.mn.us.

If you have comments about our work, or you want to suggest an audit, investigation, or evaluation, please contact us at 651-296-4708 or by e-mail at auditor@state.mn.us.


Printed on Recycled Paper

OLA
OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA • James Nobles, Legislative Auditor

February 2013

Members of the Legislative Audit Commission:

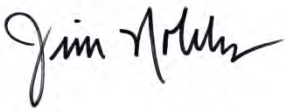
Law enforcement officers need access to information—sometimes personal and private information—to protect public safety and themselves, and some of the information they need is in state databases. There are, however, growing concerns about inappropriate use of information in certain state databases. In response to those concerns, you asked the Office of the Legislative Auditor to evaluate law enforcement's use of state databases, focusing on driver's license data and the Comprehensive Incident-Based Reporting System (CIBRS).

We concluded that the state's overall approach to managing law enforcement's use of state databases is reasonable. In that approach, the state uses data classifications, access and use restrictions, training, and monitoring to control use and guard against misuse. Nevertheless, our report highlights significant problems that need to be addressed.

We make recommendations—primarily to the Department of Public Safety—to strengthen the mechanisms that are used to manage access to driver's license data and CIBRS. We also encourage leaders in law enforcement agencies to ensure that their personnel comply with laws and policies that govern access to state databases.

This evaluation was researched and written by Carrie Meyerhoff (evaluation manager) and Matt Schroeder. We received the full cooperation of the Minnesota Department of Public Safety, assistance from many law enforcement officials, and helpful input from other interested parties. We thank them for their participation.

Sincerely,



James Nobles
Legislative Auditor

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

Table of Contents

List of Exhibits

Summary

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. (p. 19)

- 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. (pp. 45, 54)

- 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. (pp. 23-25)

- 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. (pp. 27, 29)

- 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. (pp. 34, 39)

- Law enforcement personnel have used CIBRS in ways that statutes do not permit. (p. 57)

- 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. (pp. 60, 63)

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. (p. 32)

- DPS should strengthen controls over access to driver's license information, particularly access through the DVS Web site. (p. 33)

- 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. (p. 41)

- BCA should ensure that only certified users have access to CIBRS and should explicitly address in training the recurring misuses of CIBRS. (pp. 60, 62)

- BCA should improve implementation of its CIBRS audit program and use the system's audit trail to identify inappropriate use between audits. (p. 66)

- 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. (p. 53)

Report Summary

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

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

[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.

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 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.

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

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

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

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. 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.

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

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.

Introduction

Law enforcement agencies use a wide variety of information to protect public safety and enforce the law. Some of the information law enforcement personnel access is in state databases that contain a significant amount of personal data.

Legislators, law enforcement representatives, and advocates for protecting privacy and civil liberties have struggled at times to balance competing interests and needs related to law enforcement's collection and use of data. Several recent examples highlight this struggle. During 2012, legislators considered a bill to classify certain law enforcement data as confidential, while other groups considered policy options for sharing law enforcement data with a national database and classifying law enforcement license plate reader data. In addition, beginning in 2011, media reports covered an incident of alleged widespread misuse of driver's license data by law enforcement personnel and the subsequent lawsuit.

In March 2012, the Legislative Audit Commission directed the Office of the Legislative Auditor to evaluate law enforcement's use of state databases, focusing on the driver's license database and the Comprehensive Incident-Based Reporting System, or CIBRS. The Department of Public Safety (DPS) provides Minnesota's law enforcement agencies with access to driver's license data and CIBRS. The state driver's license database contains information about every person who has a Minnesota driver's license or identification card. 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. We addressed the following questions:

- **What information do the driver's license database and CIBRS contain? How do law enforcement professionals use these databases, and is their use consistent with the law?**

- **To what extent does the Department of Public Safety (DPS) ensure that only authorized law enforcement professionals access driver's license data and CIBRS, and only for authorized purposes?**

- **How effective are procedures used by DPS to audit use of these databases? What have investigations of possible misuse found, and what have been the consequences for inappropriate use?**

- **What mechanisms has the Legislature used to balance policy issues related to law enforcement data?**

We conducted extensive data analysis to gain an understanding of the data contained in CIBRS, as well as law enforcement professionals' use of driver's license data and CIBRS. We visited several law enforcement agencies to gain

additional insights into how law enforcement personnel use driver's license and CIBRS data in their work.[1] We reviewed DPS audit files and analyzed audit trail data to identify inappropriate use of the databases.

We evaluated DPS's policies and practices for providing training, managing access, and monitoring law enforcement use of these databases by comparing them to generally accepted practices for working with personal data. We identified these generally accepted practices by reviewing publications by organizations with experience managing and protecting sensitive data.

We identified policy issues and concerns through group discussions with state and local law enforcement officials and interviews with other interested parties. We also attended policy discussions about current law enforcement data issues, reviewed documents related to past discussions, and read state and federal laws and rules and other documents.

We focused our evaluation on the Legislature's and the Department of Public Safety's roles in managing law enforcement's use of state databases. Evaluating the efforts of chief law enforcement officers to promote appropriate use of driver's license and CIBRS data was beyond the scope of our work. Thus, our findings and recommendations are primarily directed toward DPS; we did not identify strengths and weaknesses in local practices.

During our evaluation, individuals raised many issues that we did not address. These included, for example, that law enforcement agencies may be keeping data of which the public is not aware; that agencies collect too much (or too little) information; that law enforcement agencies are not collecting sufficient data on the race of persons with whom they interact; and that agencies define incidents differently, leading to inconsistent data availability and transparency. Finally, Minnesota's approach to classifying government data was a recurring topic during the evaluation.[2] Our decision not to pursue these issues reflects the feasibility of doing so given the primary focus of the evaluation, rather than a determination that the issues are unimportant.

[1] See the Appendix for a list of agencies we visited.

[2] The Minnesota Government Data Practices Act (*Minnesota Statutes* 2012, chapter 13) classifies data as public or not public. The chapter incorporates several other sections of state statutes. In addition, federal laws and agency declarations can affect data classification.

1 Background

Law enforcement agencies collect, create, and share information to protect public safety. At the same time, law enforcement professionals and policy makers must balance public safety needs with civil liberties, transparency, and privacy concerns. We begin this chapter by discussing the range of databases currently used by Minnesota law enforcement agencies and how the state makes databases available for law enforcement use. Next, we present policy issues relevant to law enforcement's use of state databases and discuss tools that can be used to balance conflicting needs and interests. We conclude with an overview of how the Legislature has used these tools to address concerns related to law enforcement's use of driver's license data and the Comprehensive Incident-Based Reporting System (CIBRS), the databases that are the focus of Chapters 2 and 3.

DATABASES AVAILABLE TO LAW ENFORCEMENT AGENCIES

Law enforcement agencies need access to information—public and not public—to do their work.

Exhibit 1.1 provides a brief description of several databases used by Minnesota law enforcement agencies in their efforts to protect public safety. As the exhibit indicates, these databases are made available by the state, the federal government, law enforcement agencies themselves, and private-sector businesses.

Most of the databases listed in Exhibit 1.1 contain information that is created by criminal justice agencies. For example, Minnesota's Computerized Criminal History integrates arrest data from law enforcement agencies, convictions and court dispositions from the courts, and probation and custody information from correction facilities and probation agencies. The Minnesota Hot Files contain data about wanted persons, and CIBRS contains information submitted by law enforcement agencies about incidents they have entered in their local records systems. Minnesota law enforcement agencies can also access Federal Bureau of Investigation databases containing criminal justice information from other states' Hot Files and criminal history data.

To aid their work, law enforcement agencies in Minnesota may also maintain their own databases. For example, computer-aided dispatch records and records management systems keep records of law enforcement activities. These data systems, and the information in them, may be shared among various jurisdictions. For example, a police department might participate with other law enforcement agencies in a regional records management system.

Finally, law enforcement personnel use databases that contain information collected and maintained by non-criminal justice agencies. For example, the Driver and Vehicle Services Division (DVS) in the Department of Public Safety (DPS) maintains and makes available for law enforcement use databases containing driver's license and motor vehicle information. In addition, private

Exhibit 1.1: Selected Databases Used by Law Enforcement

Data Source	Selected Contents
State	
CIBRS	Data on incidents and involved persons and property
Computerized Criminal History	Data on selected arrests, convictions, and sentences of persons
Driver's license data	Demographic information, photograph, and driving record of cardholders
Minnesota Hot Files	Lists of wanted persons, gang members, and protection orders
Minnesota Repository of Arrest Photographs	Booking photographs with demographic information on arrested persons
Motor vehicle data	Information on license plate numbers, owners, and registration statuses of vehicles
Predatory Offender Registry	List of persons registered as predatory offenders and all associated addresses and vehicles
Federal	
Hot Files	Lists of wanted persons, stolen property, and suspected terrorists
Interstate Identification Index	Criminal history records from FBI and other states
International Justice and Public Safety Network	Driver's licenses and vehicle registrations from other states, Canada, and Mexico
Law Enforcement Agencies	
Computer-aided dispatch systems	Requests for service and any information included in request
License plate reader data	License plate numbers scanned by agency cameras, including where they were scanned
Records management systems	Descriptions of responses to requests for service, including narratives
Suspect files	Information on suspected criminals
Commercial	
Various	Personal information such as addresses, phone numbers, relatives, associates, and property

NOTES: The Bureau of Criminal Apprehension makes the state and federal databases available to law enforcement agencies via the state's secure Criminal Justice Data Communications Network. The Driver and Vehicle Services Division also provides law enforcement agencies with access to Minnesota driver's license data and motor vehicle data through a Web site.

SOURCE: Office of the Legislative Auditor.

Government agencies and private vendors make numerous sources of data available to law enforcement agencies.

vendors make commercial databases available that can contain information unavailable through government databases, such as cell phone numbers and carriers, credit ratings, and utilities accounts. Commercial databases can also provide names and contact information for relatives and associates of persons of interest.

To make state and federal databases relatively easy to use, DPS's Bureau of Criminal Apprehension (BCA) provides systems that coordinate and automate

access.[1] For example, the Law Enforcement Message Switch allows law enforcement personnel to enter a license plate number into a computer and automatically receive information from vehicle registration data and lists of stolen vehicles, as well as information about the vehicle's registered owner from driver's license data and lists of wanted persons. BCA's Integrated Search Service enables users to enter a single set of search criteria—for instance, a last name and date of birth—and search multiple Minnesota data sources simultaneously, including criminal histories, CIBRS, driver's licenses, and court records.[2]

Law enforcement agencies use these databases for different purposes. An officer who stops a vehicle for speeding might access Minnesota and federal databases through the Law Enforcement Message Switch to learn whether the vehicle is stolen or unregistered and whether the driver has any outstanding warrants, is unlicensed, or has committed driving-related offenses in the past. The officer might add the details of this incident to his or her agency's database; depending on the database features, that information might be available to other officers who use that database.

Some law enforcement officers may use other databases for criminal investigations. For example, if a detective investigating an assault case had a suspect identified as "Joe from 13th Street," the detective could search CIBRS for other incidents involving a person fitting those characteristics. The detective might also use a commercial database to search utility records, property deeds, and other address files for a "Joe" living on "13th Street." With more complete identifying information, the detective could search state and federal criminal history databases to examine whether the suspect had been arrested for similar offenses in the past. Finally, the detective could search arrest photographs to find pictures of the suspect and other individuals similar in appearance to create a photo lineup from which witnesses could try to identify the suspect.

A law enforcement officer might use several data sources while investigating a crime.

We focused this evaluation on driver's license data and CIBRS. As Exhibit 1.2 shows, DVS and BCA make these data available to law enforcement agencies. DVS provides agencies with access to driver's license data through a Web site. BCA has also signed an agreement with DVS to provide driver's license information to agencies through the state's secure Criminal Justice Data Communications Network, which also provides agencies with access to CIBRS as well as other Minnesota and federal databases. (The Federal Bureau of Investigation provides BCA access to federal databases; BCA in turn makes these available to law enforcement agencies.)

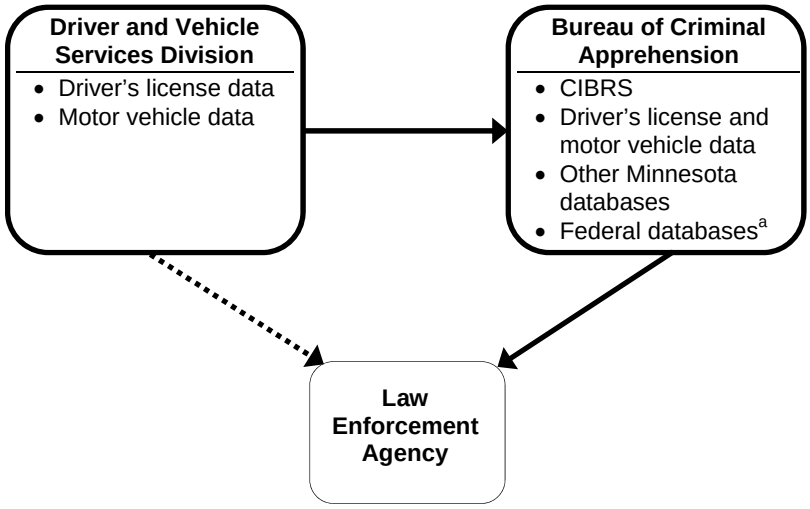
To gain access to the databases available through BCA, law enforcement agencies must sign an agreement taking responsibility for following all applicable laws and policies when accessing, using, or disseminating the data. Law enforcement agencies do not need to sign such an agreement to access driver's license data through the DVS Web site.

---

[1] BCA does not provide access to commercial databases.

[2] A user must be authorized to use these systems, and the systems will return information from only those databases the user is authorized to access. The Integrated Search Service also allows access to limited federal data.

Exhibit 1.2: Law Enforcement's Access to Databases through Department of Public Safety Divisions



[a] The Federal Bureau of Investigation provides the Bureau of Criminal Apprehension with access to federal databases and has created policies overseeing their access and use.

SOURCE: Office of the Legislative Auditor.

The Department of Public Safety (DPS) makes driver's license data and the Comprehensive Incident-Based Reporting System (CIBRS) available to law enforcement agencies.

BALANCING NEEDS AND INTERESTS

The Legislature, DPS, and law enforcement agencies must consider important—and sometimes conflicting—needs and interests surrounding the collection or use of information by law enforcement personnel. Society should benefit from government agencies collecting and sharing information and implementing new technologies that make it easier to do so. At the same time, society should be protected from threats to individual privacy and civil liberties that collection and use of data can generate. These interests, listed in Exhibit 1.3, must be balanced while maintaining the transparency necessary for open government and accountability.

Balancing these interests can be difficult. If public safety were the only consideration, we might see collection and retention of data and their dissemination among law enforcement users (and only law enforcement users) limited only by practical considerations of cost, capacity, and utility. But the need to protect civil liberties—to make sure that law enforcement agencies are not collecting and using data in ways that interfere with individuals' ability to live freely within the constraints of law—requires limits on data collection and use, as well as transparency about what is collected and how. Transparency and

Exhibit 1.3: Needs and Interests in Law Enforcement Use of State Databases

Public Safety—Law enforcement personnel need information to enforce laws and investigate crimes. They also use data in their wider role of preventing crime and threats to public safety.

Civil Liberties—Civil liberties comprise the freedom to act within the constraints of law without government interference. They include freedoms of speech, association, movement, and expression, among others.

Transparency—Outside access to information created or maintained by government agencies contributes to transparency that helps the public hold government agencies, elected officials, and others accountable. Information created and collected by law enforcement agencies can provide a record of their actions.

Individual Privacy—Individual privacy includes the ability of an individual to control his or her own personal information. Basic principles to protect personal privacy include, for example, that an individual must have a way to find out what information government has about him or her and how the information is used.[a]

[a] For additional "Fair Information Practice Principles," see *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*, (Washington, DC, 1973).

SOURCE: Office of the Legislative Auditor.

Law enforcement use of personal information raises important concerns that must be addressed.

limits on data collection could impact the ability of law enforcement agencies to do their work, however. In addition, transparency could reduce individual privacy by making personal information available to the public.

The Legislature has employed various mechanisms that can help balance these needs and interests, including (1) rules about data collection and retention, (2) data classification, (3) restrictions about access to data and their use, and (4) requirements for training or audits. With the exception of data classification, DPS and law enforcement agencies can use these mechanisms as well. In the following sections, we discuss how the Legislature has used each mechanism, while noting the roles of DPS and law enforcement agencies in implementing them. We conclude with comments about the cumulative impact of these mechanisms.

Data Collection and Retention

State statutes include guidance for government agencies about data collection and a process for disposing of government records. Statutes focus on collecting and maintaining only information that is necessary to accomplish an agency's work and support accountability. In general, the Legislature has left government agencies, including law enforcement agencies, with discretion over what the guidance means in terms of the programs each agency administers.

The Legislature requires government agencies to create and maintain "records necessary to a full and accurate knowledge of their official activities."[3] At the same time, statutes direct agencies to limit the collection and storage of data on individuals to what is "necessary for the administration and management" of government programs.[4] In some cases, the Legislature has specified data that government agencies must collect. For example, statutes state that whenever a law enforcement officer investigates an allegation of domestic violence, the officer "shall make a written report of the alleged incident."[5]

State law requires government agencies to establish retention schedules for their government records, subject to the approval of a Records Disposition Panel.[6] Not all government data are government records, however. According to state law, government records include items made or received "pursuant to state law or in connection with the transaction of public business."[7] But they do not include, for example, data and information that are not part of an official transaction.[8] The Legislature has not defined what an "official transaction" is.

Under state law, government agencies need to collect and retain data necessary to do their work and support accountability.

The Legislature has created more precise collection and retention provisions for specific state law enforcement databases. For example, state law regarding BCA's criminal gang investigative data system specifies criteria that must be met before an agency can submit data on an individual to the system (thereby controlling collection) and provides for a timeframe within which data in the system must be destroyed.[9]

Within general statutory guidance and unless otherwise specified in the law, individual law enforcement agencies have discretion over data collection and retention. Agencies also determine which of their data are "government records" and therefore subject to the Records Disposition Panel.[10] Important considerations for data collection and retention include the extent to which the information is necessary for an agency to be able to do its work or provide a complete picture of its actions. Agency discretion has implications for state databases such as CIBRS, which contains data submitted by law enforcement agencies. Law enforcement agencies can submit only data they have collected

---

[3] *Minnesota Statutes* 2012, 15.17, subd. 1.

[4] *Minnesota Statutes* 2012, 13.05, subd. 3. *Minnesota Rules* 2007-10, sec. 1205.1500, subp. 4, provides elaboration on determining whether there is a need for data.

[5] *Minnesota Statutes* 2012, 629.341, subd. 4.

[6] *Minnesota Statutes* 2012, 138.17, subd. 7. Subd. 1(a) defines the Records Disposition Panel to include the Attorney General, the Director of the Minnesota Historical Society, and the Legislative Auditor (for state records) or State Auditor (for local records).

[7] *Ibid.*, subd. 1(b)(1).

[8] *Ibid.*, subd. 1(b)(4).

[9] *Minnesota Statutes* 2012, 299C.091, subds. 2 and 5.

[10] For more information on collection and retention of government data, see Minnesota Historical Society, *Preserving and Disposing of Government Records* (St. Paul, May 2008); and Minnesota Historical Society, *Managing Your Government Records: Guidelines for Minnesota Archives and Agencies* (St. Paul, September 2009).

and retained in their records systems. Agencies that submit data to CIBRS also have control over those data and how long they remain in CIBRS.

Data Classification

In Minnesota, the Legislature determines the classification of government data.

Government data include all information "collected, created, received, maintained or disseminated" by a government agency.[11] Data classification establishes whether the public or subjects of government data may have access to them. In Minnesota, the Legislature determines data classification. Through the Minnesota Government Data Practices Act, the Legislature has classified all government data as public unless state or federal law or temporary classification specifically designates them as not public.[12] Exhibit 1.4 shows Minnesota's data classifications.

Exhibit 1.4: Classifications for Not Public Data

Data on individuals[a]	
Private	Accessible to the individual subject, but not to the public
Confidential	Inaccessible to the individual subject and the public
Data not on individuals	
Nonpublic	Accessible to the subject, if any, but not to the public
Protected nonpublic	Inaccessible to the subject and the public

NOTE: In Minnesota, all data collected, created, received, maintained or disseminated by a government entity are public unless classified otherwise by state statute, temporary classification, or federal law.

[a] Data in which any individual is or can be identified as the subject of the data, unless (1) the appearance of the name or other identifying data can be clearly demonstrated to be only incidental and (2) the data are not accessed by the name or other identifying data of any individual.

SOURCE: *Minnesota Statutes* 2012, 13.02, subds. 3, 5, 9, 12, and 13; and 13.03, subd. 1.

Minnesota law establishes the presumption that government data are public unless classified otherwise.

A presumption that government data are public can contribute to government transparency and accountability. At the same time, this presumption can create privacy or public safety concerns. The Legislature has addressed some privacy concerns by classifying some government data as not public. For example, welfare data are presumptively private.[13] A person who is the subject of private data can access the data, but the general public cannot. The Legislature has also provided a means by which government agencies can seek temporary classification of data

[11] *Minnesota Statutes* 2012, 13.02, subd. 7.

[12] *Minnesota Statutes* 2012, 13.03, subd. 1. *Minnesota Statutes*, chapter 13, is the state's Government Data Practices Act. Although we focus our discussion on data classification, the act includes many other elements, such as provisions giving individuals the ability to challenge the accuracy and completeness of certain data about themselves.

[13] *Minnesota Statutes* 2012, 13.46, subd. 2.

as not public.[14] Finally, the Legislature has accommodated some public safety concerns that might arise when data are available to the general public or individuals who are the subject of the data. For example, with some exceptions, personal information that is part of an active criminal investigation is confidential,[15] and law enforcement agencies can withhold public data in some circumstances.[16]

An important consideration in classifying government data is how much the data reveal about a person. Technology heightens this consideration by increasing government's capacity to collect, store, and analyze information. Individual pieces of information might reveal little about a person, but in combination with other information or over time they might threaten individual privacy. The idea that individuals have a privacy interest in compilations of public data is relevant to state databases and may lead to the same information being classified differently in different contexts.[17] For example, generally, personal data in a local law enforcement agency's incident reports are public, but they are private in CIBRS.[18]

Classification of law enforcement data is particularly complicated.

Among all government data, the classification of law enforcement data is especially complicated. The Legislature has made distinctions based on the stage of the investigative process, potential consequences of releasing information, and type of crime, among other things. For example, while some data are public at the local law enforcement agency, other information about an event may be private or confidential if (1) it is part of an active criminal investigation, (2) its release might endanger someone or cause a suspect to flee, or (3) it identifies a victim of criminal sexual conduct.[19]

DPS and law enforcement agencies must follow the Minnesota Government Data Practices Act regarding data they collect, create, maintain, use, or disseminate.[20] For example, as illustrated in Exhibit 1.2, DVS creates driver's license

---

[14] *Minnesota Statutes* 2012, 13.06. Government entities achieve temporary classification of data through application to the Commissioner of Administration. If the temporary classification is granted by the Commissioner and approved by the Attorney General, it lasts until August of the year following the year it is presented to the Legislature for consideration. The Commissioner is required to present all temporary classifications to the Legislature on or before January 15.

[15] According to *Minnesota Statutes* 2012, 13.82, subd. 7, a criminal investigation becomes inactive upon: "(a) a decision by the agency or appropriate prosecutorial authority not to pursue the case; (b) expiration of the time to bring a charge or file a complaint under the applicable statute of limitations, or 30 years after the commission of the offense, whichever comes earliest; or (c) exhaustion of or expiration of all rights of appeal by a person convicted on the basis of the investigative data."

[16] *Minnesota Statutes* 2012, 13.82, subds. 7, 14, and 17.

[17] For a case articulating this privacy interest, see U.S. Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989).

[18] *Minnesota Statutes* 2012, 299C.40, subd. 4. Some data that are part of an active criminal investigation are classified as confidential in CIBRS and at the local agency. See also, *Minnesota Statutes* 2012, 13.82, subd. 7.

[19] *Minnesota Statutes* 2012, 13.82, subds. 6, 7, 14, and 17.

[20] See, for example, *Minnesota Statutes* 2012, 13.025; 13.03, subd. 2; 13.04, subds. 3 and 4; and 13.05. See also, *Minnesota Rules* 2007-10, secs. 1205.0800 through 1205.1500.

information. Through an intra-agency agreement, DVS provides BCA with access to these data. The agreement includes a clause mandating DVS and BCA compliance with the act. BCA, in turn, makes these data available to law enforcement agencies, which sign an agreement mandating their compliance with the act.

Access and Use Restrictions

Restrictions on who may access information and the purposes for which the information may be used can help protect civil liberties and address privacy concerns while meeting public safety needs for information.

To help balance public safety needs and privacy interests, law enforcement agencies must limit access to and use of data to what is necessary for their work.

Taken as a whole, general provisions of state law related to government use of data limit use—and arguably access—to that which is necessary to conduct government functions. State law says that government agencies should limit their use of private and confidential data on individuals to what is necessary for the administration and management of government programs.[21] In addition, the law limits the use of private and confidential data to those purposes (1) stated to the individual at the time the agency collected the data or (2) otherwise allowed by law.[22] The Legislature has made an allowance for law enforcement agencies related to use of private and confidential data: state law clarifies that nothing in the Minnesota Government Data Practices Act "prohibits the exchange of information by law enforcement agencies" if it is needed for an investigation.[23]

In some cases, the Legislature has created access and use restrictions for specific state databases used by law enforcement personnel. Both driver's license photographs and CIBRS data provide examples of this. As we discuss in more detail in Chapters 2 and 3, the permissible uses of these data are outlined in statutes.[24] In addition, the Legislature has restricted CIBRS access to only trained and certified individuals in eligible Minnesota law enforcement agencies.[25]

DPS and law enforcement agencies have roles in ensuring law enforcement personnel's appropriate access to and use of state databases. Law enforcement agencies are responsible for determining which of their personnel need access to what information. DPS can set up access to the state databases it manages in accordance with agencies' specifications.

---

[21] *Minnesota Statutes* 2012, 13.05, subd. 3.

[22] *Ibid.*, subd. 4. *Minnesota Statutes* 2012, 13.04, subd. 2, requires government agencies, when they ask individuals for private or confidential information, to inform the individuals of the purpose for collecting the data and the uses to which the data will be put. Law enforcement officers are not required to provide this information, known as the Tennessen Warning, when they request information to build a criminal case.

[23] *Minnesota Statutes* 2012, 13.82, subd. 24.

[24] *Minnesota Statutes* 2012, 171.07, subd. 1a; and 299C.40, subd. 2.

[25] *Minnesota Statutes* 2012, 299C.40, subds. 1(c) and 5.

Training and Audits

Training and audit requirements are mechanisms to ensure that collection and retention rules, data classification, and access and use restrictions are understood and followed. As such, they can help achieve balance among policy issues. Training increases the likelihood that persons who access and use government data understand their classification and any use restrictions. Audits can verify compliance or provide opportunities for correction when rules and restrictions are not being followed.

In some cases, the Legislature requires training or audits related to state databases. For example, the CIBRS section of statutes implies that BCA must train system users and directs BCA to maintain an audit trail of all CIBRS transactions.[26] As another example, state law requires BCA to audit data submitted to the criminal gang investigative data system it maintains.[27] DPS and law enforcement agencies might use training and internal audits to manage employees' use of state databases, even absent statutory requirements to do so.

Reasonable approaches to balancing needs and interests can be difficult to manage in practice.

Cumulative Impact of Mechanisms

Mechanisms that provide reasonable approaches to balance conflicting needs and interests related to law enforcement's use of a particular database can become unmanageable in combination with others. As we discussed in the beginning of this chapter, law enforcement personnel have access to multiple data sources. The associated data classifications, access and use restrictions, and training and audit requirements risk creating a web of regulation that can be difficult for law enforcement agencies to manage. Some law enforcement officials told us that managing multiple sources of data is challenging. Varying regulations could also create circumstances in which knowledgeable and responsible users mistakenly use databases for work-related purposes that are not permitted.

EVALUATION FOCUS

This evaluation focuses on state controls over law enforcement's use of driver's license data and CIBRS data. Exhibit 1.5 shows the statutory framework for those controls. Statutes require DPS to collect driver's license data and specify data classification and use restrictions for them. The CIBRS section of statutes includes data classification, access and use restrictions, and training and audit trail requirements. In the following chapters, we describe and evaluate the Department of Public Safety's management of law enforcement's use of driver's license and CIBRS data. We also offer an overall assessment of how the state has balanced the policy interests surrounding law enforcement use of these two databases.

---

[26] *Minnesota Statutes* 2012, 299C.40, subds. 4(h) and 5. While statutes require an audit trail, they do not require audits.

[27] *Minnesota Statutes* 2012, 299C.091, subd. 4.

Exhibit 1.5: Statutes that Balance Needs and Interests Related to Driver's License and CIBRS Data

	Driver's License Data	CIBRS Data
Collection and Retention		
Collection	*Minnesota Statutes* 2012, 171.12, subd. 1(a)	None
Retention	None	None
Data Classification	*Minnesota Statutes* 2012, 171.07, subd. 1a; and 171.12, subd. 7	*Minnesota Statutes* 2012, 299C.40, subd. 4
Access and Use		
Access	None	*Minnesota Statutes* 2012, 299C.40, subds. 1(c) and 5
Use	*Minnesota Statutes* 2012, 171.07, subd. 1a; and 171.12, subd. 7	*Minnesota Statutes* 2012, 299C.40, subd. 2
Training and Audits		
Training	None	*Minnesota Statutes* 2012, 299C.40, subd. 5
Audit trail	None	*Minnesota Statutes* 2012, 299C.40, subd. 4(h)
Audits	None	None

NOTES: Exhibit reflects mechanisms in *Minnesota Statutes* that specifically address driver's license or CIBRS data. CIBRS is the Comprehensive Incident-Based Reporting System. General statutory provisions, such as the Minnesota Government Data Practices Act, speak to some of these mechanisms for all government data. The Department of Public Safety and individual law enforcement agencies may employ additional tools.

SOURCE: Office of the Legislative Auditor.

2 Driver's License Data

The Driver and Vehicle Services Division (DVS) in the Department of Public Safety (DPS) maintains information about Minnesota drivers, driving records, and vehicle registrations. The division makes this information available to law enforcement professionals, as well as others, for certain purposes. In late 2011, media reported a case of numerous law enforcement personnel accessing a person's driver's license information, possibly for non-work-related purposes.[1] Inappropriate access to driver's license information was not a new phenomenon and has involved users outside of law enforcement. However, the scope of the alleged misuse and publicity surrounding it and the resulting lawsuit brought visibility to misuse specifically by members of law enforcement.

The Driver and Vehicle Services Division (DVS) collects, maintains, and disseminates driver's license information.

We begin this chapter by providing background information about driver's license data, including their permissible uses and common uses by law enforcement personnel. Next, we discuss inappropriate use of driver's license data. We then evaluate how DPS has trained users on the appropriate uses of and managed access to the data, and assess the department's monitoring activities. We conclude with remarks about how the state's management of driver's license data for law enforcement use balances the policy interests we discussed in Chapter 1.

BACKGROUND

Driver's license information includes a driver's name, date of birth, address, height, and weight, as well as the driver's license number and status.[2] Information also includes drivers' current and historical driver's license photographs. We focused on this personal information and not on vehicle registration information and driving records that DVS maintains. In the following sections, we provide information on the classification and permissible uses of driver's license information, before focusing on its use by law enforcement personnel.

Data Classification and Permissible Uses

As Exhibit 2.1 shows, personal driver's license information maintained by DVS includes public and private data.[3] Minnesota law classifies government data as public if they are not classified otherwise by state or federal law or temporary

[1] See, for example, Paul Blume, "DVS Database Searches of Woman's History May be Data Breach," October 3, 2011, http://www.myfoxtwincities.com/story/17616852/dvs-database-searches-of-womans-history-may-be-data-breach, accessed December 31, 2012.

[2] Throughout, our reference to driver's license data also includes state identification cards.

[3] Private data are available to the subject of the data, but not the general public.

classification.[4] Federal law provides the basis for classifying some driver's license information as private. The federal Driver's Privacy Protection Act identifies several pieces of driver's license information as "personal information" and restricts their release by state departments that collect and maintain them.[5] For example, federal law identifies driver's license numbers and addresses as personal information.

Under the federal Driver's Privacy Protection Act, most driver's license information is private.

Exhibit 2.1: Classification of Driver's License Data Maintained by the Driver and Vehicle Services Division

	Public	Private
Address (excluding 5-digit zip code)		X
Date of birth		X
Designated caregiver information		X
Driver's license number		X
Driver's license photograph		X
Driver's license status	X	
Medical data		X
Personal name		X
Physical description	X	
Social Security number		X
Zip code (5-digit)	X	

SOURCE: Minnesota Department of Public Safety, Driver and Vehicle Services eLearning for Law Enforcement, "Classifications of Data Held by the Driver and Vehicle Services Division," abridged by the Office of the Legislative Auditor, and *18 U.S. Code*, sec. 2725 (2006).

The act defines permissible uses of driver's license information.

Congress passed the Driver's Privacy Protection Act in 1994 after a woman was murdered by a man who obtained her address from a private investigator who got the address from motor vehicle information. As originally passed, the act allowed states to release driver's license information as long as they provided a means for individuals to "opt out" of its release. Thus, until 2000, Minnesota classified driver's license information, except for the photograph, as public unless individuals "opted out." Congress amended the act in 1999, changing the permissible uses that allowed Minnesota to classify the data as public to a requirement that a driver affirmatively agree ("opt in") to the release of his or her data in response to a request or for marketing purposes.

The Driver's Privacy Protection Act identifies "permissible uses" for which state driver's license agencies may release personal information.[6] As Exhibit 2.2 shows, permissible uses go beyond law enforcement activities and include other government and private sector uses. A subset of personal information—labeled

[4] *Minnesota Statutes* 2012, 13.03, subd. 1.

[5] *18 U.S. Code*, secs. 2721-5 (2006).

[6] *18 U.S. Code*, sec. 2721 (2006). The law also identifies uses for which the data must be released by states.

Exhibit 2.2: Permissible Uses of Driver's License Information Under Federal Law

	Highly Restricted Personal Information[a]	Other Personal Information[b]
For use by any government agency, including any court or law enforcement agency, in carrying out its functions.	X	X
For use in connection with matters of motor vehicle safety, theft, emissions, product alterations, recalls, advisories, performance monitoring, parts, dealers, and market research activities; driver safety; and removal of non-owner records from the original owner records of motor vehicle manufacturers.		X
For use in the normal course of business by a legitimate business, but only (A) to verify the accuracy of personal information submitted by the individual to the business; and (B) if such information as so submitted is not correct or is no longer correct, to obtain the correct information, but only for the purposes of preventing fraud by, pursuing legal remedies against, or recovering on a debt or security interest against, the individual.		X
For use in connection with any civil, criminal, administrative, or arbitral proceeding.	X	X
For use in research activities, and for use in producing statistical reports, so long as the personal information is not published, redisclosed, or used to contact individuals.		X
For use by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in connection with claims investigation activities, antifraud activities, rating, or underwriting.	X	X
For use in providing notice to the owners of towed or impounded vehicles.		X
For use by any licensed private investigative agency or licensed security service for any purpose permitted under this subsection.		X
For use by an employer or its agent or insurer to obtain or verify information relating to a holder of a commercial driver's license.	X	X
For use in connection with the operation of private toll transportation facilities.		X
For any other use in response to requests for individual motor vehicle records if the State has obtained the express consent of the person to whom such personal information pertains.		X
For bulk distribution for surveys, marketing or solicitations if the State has obtained the express consent of the person to whom such personal information pertains.		X
For use by any requester, if the requester demonstrates it has obtained the written consent of the individual to whom the information pertains.		X
For any other use specifically authorized under the law of the State that holds the record, if such use is related to the operation of a motor vehicle or public safety.		X

[a] "Highly restricted personal information" includes: photograph, Social Security number, and medical or disability information.

[b] "Other personal information" includes: driver identification number, name, address (but not 5-digit zip code), and telephone number.

SOURCE: *18 U.S. Code*, secs. 2721 and 2725 (2006), abridged by the Office of the Legislative Auditor.

"highly restricted personal information"—may be released for only 4 of the 14 permissible uses.[7]

State statutes declare that DPS shall treat driver's license data as provided by federal law.[8] State statutes also direct DPS to disclose driver's license information

[7] *18 U.S. Code*, secs. 2721 and 2725 (2006). "Highly restricted personal information" includes the photograph, Social Security number, and medical or disability information.

[8] *Minnesota Statutes* 2012, 171.12, subd. 7(a). Specifically, Minnesota law says the data shall be treated as provided by federal law in effect on May 23, 2005.

"where the use is related to the operation of a motor vehicle or to public safety."[9] Minnesota statutes address use of driver's license photographs separately from other personal driver's license information. As shown in Exhibit 2.3,

- **Minnesota law limits permissible uses of driver's license photographs more than federal law.**

In 1981, the Legislature classified driver's license photographs as private data and restricted their use to issuance of driver's licenses and investigation and prosecution of felonies.[10] Over time, the Legislature has expanded the allowed uses of driver's license photographs, but they are still narrower than what federal law allows. For example, state law limits law enforcement uses of photographs to the investigation and prosecution of crimes and other listed uses.[11] In contrast, federal law would permit use "by any government agency, including any court or law enforcement agency, in carrying out its functions."[12]

Minnesota law limits the use of driver's license photographs more than other driver's license information.

Exhibit 2.3: Permissible Uses of Driver's License Photographs

State Law	The use of driver's license photographs maintained by the Department of Public Safety is restricted to: • the issuance and control of drivers' licenses; • criminal justice agencies…for the investigation and prosecution of crimes, service of process, enforcement of no contact orders, location of missing persons, investigation and preparation of cases for criminal, juvenile, and traffic court, and supervision of offenders; • public defenders…for the investigation and preparation of cases for criminal, juvenile, and traffic courts; and • child support enforcement purposes.
Federal Law	Without the express consent of the person to whom such information applies, the use of driver's license photographs is restricted to: • use by any government agency, including any court or law enforcement agency, in carrying out its functions…; • use in connection with any civil, criminal, administrative, or arbitral proceeding…; • use by any insurer or insurance support organization…in connection with claims investigation activities, antifraud activities, rating, or underwriting; and • use by an employer or its agent or insurer to obtain or verify information relating to a holder of a commercial driver's license….

SOURCES: *Minnesota Statutes* 2012, 171.07, subd. 1a; and *18 U.S. Code,* secs. 2721 and 2725 (2006).

[9] *Minnesota Statutes* 2012, 171.12., subd. 7a. This subdivision says the information is "related to public safety if it concerns the physical safety or security of drivers, vehicles, pedestrians, or property."

[10] *Laws of Minnesota* 1981, chapter 363, sec. 37.

[11] *Minnesota Statutes* 2012, 171.07, subd. 1a.

[12] *18 U.S. Code,* sec. 2721(b)(1) (2006).

Law Enforcement Use

Law enforcement agencies make extensive use of driver's license data as they enforce laws, investigate crimes, and complete other public safety work.

Law enforcement personnel use driver's license information for many work-related purposes. For example, a patrol officer might access driver's license information to verify the license status and identity of a driver who left his or her license at home. Civilian staff might check the driver's license information and photograph of a person to whom the sheriff's office must serve court documents. A police lieutenant might display the driver's license photograph of a wanted person to officers for identification purposes. A records clerk might use driver's license information to correct or complete information in a police report. An investigator might look up a suspect's driver's license photograph to confirm the suspect's identity. Several law enforcement representatives noted the importance of the driver's license photograph for confirming identities.

Law enforcement users can access driver's license information through a DVS Web site, systems provided by the Bureau of Criminal Apprehension (BCA), or both.[13] We found:

- **Law enforcement personnel accessed driver's license information extensively in fiscal year 2012.**

More than 11,000 law enforcement personnel used the DVS Web site to access driver's license information during fiscal year 2012, performing about 3.8 million queries.[14] The median number of queries per law enforcement user that year was around 170; the user with the most queries performed nearly 11,500 queries during the year. Law enforcement users accessed driver's license data of 1.46 million individuals through the DVS Web site. Most of these individuals (55 percent) were queried just once during the 12 months.

Law enforcement personnel used BCA systems even more often to access driver's license information.[15] The record of queries through BCA systems does not lend itself to analyses like those above, so we asked BCA for the total number of law enforcement queries of driver's license demographic information and photographs for two three-month periods. Between January and March 2012, law enforcement personnel performed more than three times as many

---

[13] For the most part, we considered law enforcement users to be personnel in agencies listed in *Minnesota Statutes* 2012, 299C.40, subd. 1(c). Those agencies include Minnesota municipal police departments, the Metropolitan Transit Police, the Metropolitan Airports Police, the University of Minnesota Police Department, the Department of Corrections Fugitive Apprehension Unit, Minnesota county sheriff's departments, the Enforcement Division of the Department of Natural Resources, the Bureau of Criminal Apprehension, and the Minnesota State Patrol. The DVS audit trail data we analyzed excluded one such agency and included agencies not specifically listed.

[14] DVS records queries of driver's license data such that each record may not represent an intentional request for data. Each record reflects the hour and minute of the query. To estimate a user's intentional queries, we did *not* count queries that occurred within one minute of a query of the exact same information, unless there was a possibility of intervening queries of other information. The total number of records in the DVS data was 3 percent higher than our estimated number of intentional queries.

[15] BCA provides law enforcement personnel with access to driver's license data through the Law Enforcement Message Switch and Integrated Search Service.

queries of driver's license information through BCA systems as they performed through the DVS Web site (almost 3 million queries versus about 920,000).[16]

Means of Accessing Driver's License Information

Law enforcement personnel access driver's license data through a DVS Web site or systems provided by the Bureau of Criminal Apprehension (BCA).

Both the DVS Web site and BCA systems allow users to search for information based on license plate number, driver's license number, or name and date of birth. The means by which an individual user accesses the information might depend on ease of use, information needs, technical considerations, and preferences.

According to some law enforcement users, the DVS Web site has search flexibility that is not easily available with the BCA systems. Specifically, the DVS Web site allows a law enforcement user to search for information about a person when only a partial name is known.

The two means of access also return different information. The DVS Web site provides information on a driver's record, registered vehicles, and current and historical driver's license photographs. Exhibit 2.4 shows an example of a fictional driver's information returned by the DVS Web site. The driver's demographic information is displayed at the top of the screen, with tabs for viewing additional information, such as motor vehicle information.

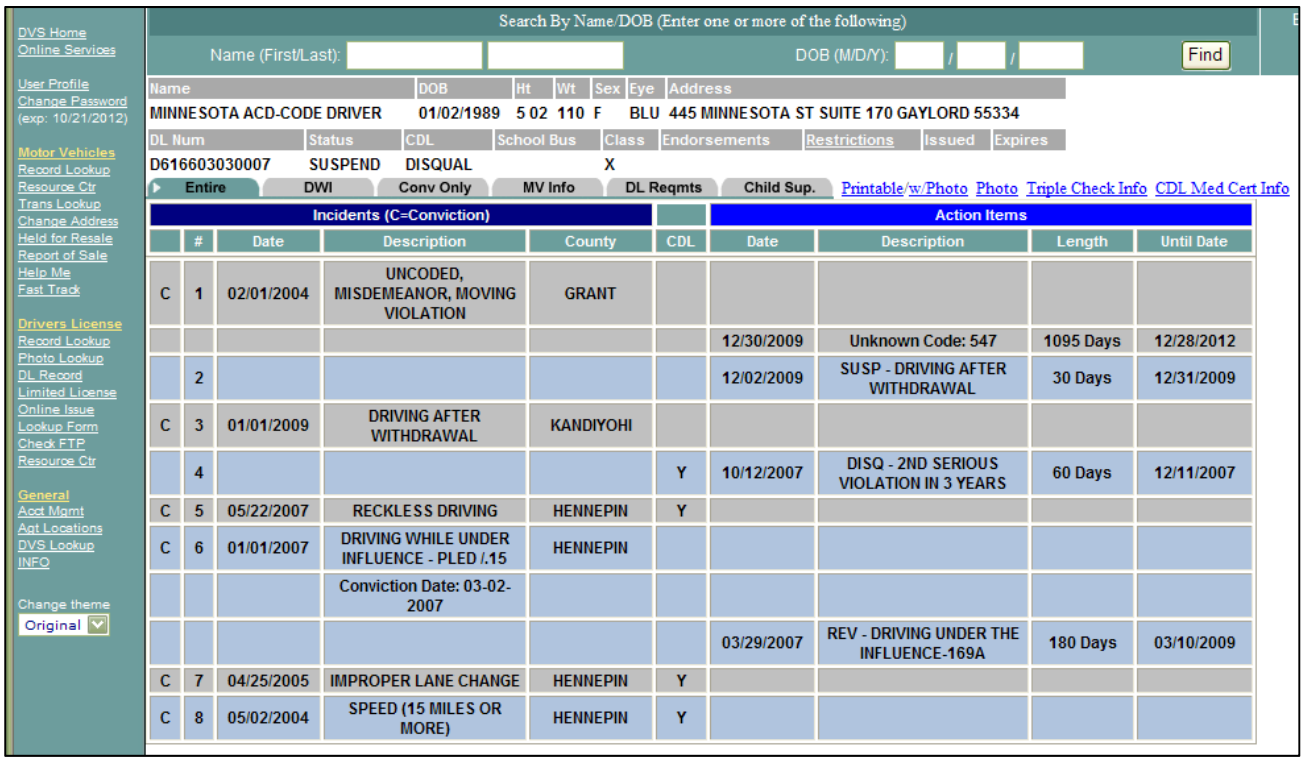
Compared to the DVS Web site, the BCA systems return less information about a driver's record and display, at most, only the current photograph.[17] An advantage of the BCA systems is that law enforcement personnel can use them to quickly compare driver and vehicle information against other databases, such as "hot files" listing wanted persons or vehicles. Exhibit 2.5 shows driver information displayed through BCA systems.

How sworn law enforcement officers use these two modes to access driver's license information also varies based on technical reasons or preferences. One sheriff suspected that the deputies in that agency seldom use either system in their vehicles, instead relying upon dispatchers to run information for them. Another sheriff said the agency's deputies use the DVS Web site regularly on patrol; they do not have access to BCA systems in their vehicles and rely on dispatchers to retrieve information through those systems. At a third agency, one sworn officer said that sometimes it is easier to view driver's license photographs through the DVS Web site, although he could do so through BCA systems.

[16] In the first quarter of 2011, prior to the possible inappropriate use mentioned in the introduction to this chapter, law enforcement queries through BCA were just over two times the number of queries through the DVS Web site.

[17] BCA systems provide access to the most current photograph, but some law enforcement agencies' systems may be unable to display photographs in their squad cars.

Exhibit 2.4: Driver and Vehicle Services Web Site Driver Information



DVS Home
Online Services

User Profile
Change Password
(exp: 10/21/2012)

Motor Vehicles
Record Lookup
Resource Ctr
Trans Lookup
Change Address
Held for Resale
Report of Sale
Help Me
Fast Track

Drivers License
Record Lookup
Photo Lookup
DL Record
Limited License
Online Issue
Lookup Form
Check FTP
Resource Ctr

General
Acct Mgmt
Agt Locations
DVS Lookup
INFO

Change theme
Original

Search By Name/DOB (Enter one or more of the following)

Name (First/Last): DOB (M/D/Y): Find

Name	DOB	Ht	Wt	Sex	Eye	Address
MINNESOTA ACD-CODE DRIVER	01/02/1989	5 02	110	F	BLU	445 MINNESOTA ST SUITE 170 GAYLORD 55334

DL Num	Status	CDL	School Bus	Class	Endorsements	Restrictions	Issued	Expires
D616603030007	SUSPEND	DISQUAL		X				

Entire | DWI | Conv Only | MV Info | DL Reqmts | Child Sup. | Printable/w/Photo | Photo | Triple Check Info | CDL Med Cert Info

Incidents (C=Conviction)						Action Items			
	#	Date	Description	County	CDL	Date	Description	Length	Until Date
C	1	02/01/2004	UNCODED, MISDEMEANOR, MOVING VIOLATION	GRANT					
						12/30/2009	Unknown Code: 547	1095 Days	12/28/2012
	2					12/02/2009	SUSP - DRIVING AFTER WITHDRAWAL	30 Days	12/31/2009
C	3	01/01/2009	DRIVING AFTER WITHDRAWAL	KANDIYOHI					
	4				Y	10/12/2007	DISQ - 2ND SERIOUS VIOLATION IN 3 YEARS	60 Days	12/11/2007
C	5	05/22/2007	RECKLESS DRIVING	HENNEPIN	Y				
C	6	01/01/2007	DRIVING WHILE UNDER INFLUENCE - PLED /.15	HENNEPIN					
			Conviction Date: 03-02-2007						
						03/29/2007	REV - DRIVING UNDER THE INFLUENCE-169A	180 Days	03/10/2009
C	7	04/25/2005	IMPROPER LANE CHANGE	HENNEPIN	Y				
C	8	05/02/2004	SPEED (15 MILES OR MORE)	HENNEPIN	Y				

NOTES: This screen shot illustrates the type of information visible to a law enforcement user of the Driver and Vehicle Services Web site. The screen shot does not contain actual driver's license information. We cropped the screen shot to eliminate white space and the Web site URL.

SOURCE: Driver and Vehicle Services Division, October 2012.

During our ride-along experiences, officers relied on BCA systems most to access driver's license information.[18] For example, an officer entered a license plate number from a speeding car into his mobile terminal to learn if the vehicle was registered, the registered owner had a valid license, and either the vehicle or owner was on a "hot file" list. The officers used the DVS Web site when (1) the BCA system had not returned information to the officer before he needed to approach a driver during a traffic stop, (2) a driver did not have a license with her and the officer wanted the search flexibility of the DVS Web site, (3) the officer needed to view the driver's photograph, and (4) the officer wanted to see if a driver with an out-of-state license had any driving violations in Minnesota.[19]

[18] See the Appendix for a list of the law enforcement agencies we visited during our evaluation.

[19] DVS maintains records about driving violations committed in Minnesota by drivers who do not have a Minnesota driver's license.

Exhibit 2.5: Bureau of Criminal Apprehension Systems Driver Information

```
TO: PPK-00000134 20050203 11:57:58 2404000086
FROM: A36MPQ43-02227946 20050203 11:57:58 24040000DA

TXT
NAM/POCKETS,EMMITT TEA.*RECORD DISSEMINATION RESTRICTED*
SNM/1111 E. PENNILESS LANE. CTY/MISSION. STA/MN. ZIP/10001.
SEX/M. DOB/19420426. HGT/510. WGT/180. EYE/HZL.
DISABILITY CERTIFICATES:N
OLN/M255792626396. OLT/1. CLS/D. EXP/042605
STATUS:VALID GLASSES DONOR:N DESIGNATED CAREGIVER:N
PHOTO:1697144042.ISU/061201.DNR TRAINING=FIREARM:N,SNOWMOBILE:N

08/30/01 SPEED 82 2001292
04/25/01 SPEED 18 2001149
03/26/90 REINSTATE DRIVING PRIVILEGES
03/26/90 INSURANCE ON (ACCIDENT #) 93580235
03/23/90 * SUSP - NO FAULT - ACCIDENT 00030
03/26/90 93580235
END VIOLATIONS
```

During our ride-along observations, officers relied on BCA systems more than the DVS Web site to access driver's license information.

NOTES: This image illustrates the type of information visible to a law enforcement user of Bureau of Criminal Apprehension (BCA) systems. The image, from BCA training, does not include actual driver's license information.

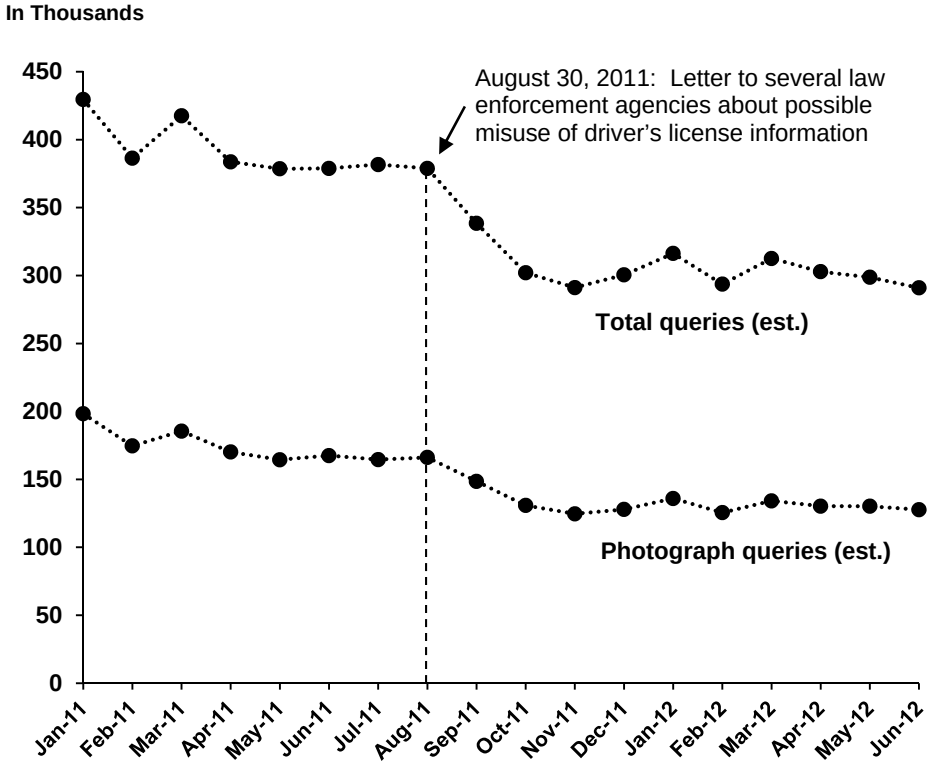
SOURCE: Bureau of Criminal Apprehension, MNJIS Training and Auditing Unit, "File Queries."

Trends in Law Enforcement Use

As Exhibit 2.6 shows, law enforcement personnel's use of the DVS Web site has decreased over the 18 months beginning January 2011. Use over the first several months generally trended down, before a relatively steep drop in fall 2011. Law enforcement users might be shifting their queries of driver's license data from the Web site to BCA systems, which showed an increase in queries between the first quarter of 2011 and the first quarter of 2012. Technology changes might explain some of the shift from the DVS Web site to BCA systems. A law enforcement officer at one agency said the agency had equipped patrol cars to access driver's license information through BCA systems only within the past year or so, and an officer at another agency said the agency had upgraded the software for its mobile systems to view driver's license photographs through BCA systems within the past year. The steep drop in use was likely a reaction to alleged misuse of the Web site that came to light around that time. That drop may reflect users correcting their misuse, growing reluctant to use the DVS Web site even for allowed purposes, or both.

In the following section, we discuss inappropriate use of driver's license information by law enforcement. Then, in later sections, we evaluate the department's policies and procedures for training users, controlling law enforcement access to driver's license information, and monitoring use.

Exhibit 2.6: Law Enforcement Queries of DVS Web Site, January 2011 – June 2012



Law enforcement use of the DVS Web site dropped noticeably after alleged misuse of the site by users from several law enforcement agencies.

NOTES: DVS records queries of driver's license data such that each record may not represent an intentional request for data. Each record reflects the hour and minute of the query. To estimate a user's intentional queries, we did *not* count queries that occurred within one minute of a query of the exact same information, unless there was a possibility of intervening queries of other information. The total number of records in the DVS data was 3 percent higher than our estimated number of intentional queries.

SOURCE: Office of the Legislative Auditor, analysis of Driver and Vehicle Services Division audit trail.

INAPPROPRIATE USE

We defined inappropriate use as accessing driver's license information with invalid access privileges or without a permissible purpose. Misuse could include non-work-related use or work-related use that is not permitted by law. Under our definition, accessing the DVS Web site using outdated access privileges is inappropriate use. So, too, is viewing information when there is not a permissible work need. Misuse is not signified by the volume of use, but rather the purpose behind it. Inappropriate use does not require malicious intent or use for personal gain. We found:

- **Some law enforcement personnel have used driver's license data inappropriately.**

Inappropriate use includes non-work-related use of the systems that provide access to driver's license data, even if the data are not disseminated or used maliciously.

We identified inappropriate access to the DVS Web site, as well as questionable uses of driver's license photographs. Most of the instances of misuse we summarize below reflect law enforcement agencies' findings as reflected in DVS and BCA audit files.[20] Although we could not quantify the full extent of inappropriate use of the DVS Web site, we analyzed records of Web site queries to get a sense of the possible magnitude of misuse.

Inappropriate use includes an individual accessing the DVS Web site under access privileges associated with an agency for which he or she no longer works. A law enforcement agency should alert DVS to disable a former employee's username and password, and the former employee should not use those credentials any longer.[21] During the 18 months ending June 30, 2012, 13 users conducted queries using access privileges associated with law enforcement agencies that no longer existed. Over the same time period, three former employees of state law enforcement agencies, as well as four former employees of local law enforcement agencies, accessed the DVS Web site using usernames and passwords that should have been disabled. Others who might have access when they do not need it are individuals whose job responsibilities have changed or who are on long-term leave.

Other examples of misuse include some of the uses of driver's license information described to us by law enforcement representatives. As Exhibit 2.7 shows, some of the uses of driver's license photographs appear to be inappropriate. These uses might be work-related, but they do not seem to fall within the uses allowed by state law.

Inappropriate use of driver's license information includes work-related uses that are not allowed by law.

Inquiries conducted by DVS and investigated by law enforcement agencies during fiscal year 2012 found that 88 law enforcement personnel had misused the DVS Web site.[22] For example, in one case, the law enforcement agency reported that the user looked up the address of a friend. In some cases, users looked up information about a co-worker or relative. Between early 2010 and May 2012, investigations of alleged misuse of data by law enforcement personnel using BCA systems revealed that six individuals misused driver or vehicle information.[23]

Besides these concrete examples of misuse, we found:

- **A significant proportion of law enforcement users may have accessed driver's license data for inappropriate purposes.**

[20] Misuse documented in DVS and BCA audit files may include inappropriate use of motor vehicle information, rather than driver's license information.

[21] It is possible that a user obtained new employment with a law enforcement agency and used his or her old username and password out of habit. In this situation, the uses of the data might have been permissible even though using old access privileges was not.

[22] We accepted the investigation outcomes reported to DVS or recorded by the division. The 88 individuals include 24 who DVS surmised had misused the Web site. One hundred forty-four instances of possible misuse were not sustained. Investigations into 94 instances of Web site use by law enforcement personnel were inconclusive or the outcomes were not known to DVS.

[23] We accepted the investigation outcomes reported to BCA. Several investigations of alleged misuse through BCA systems were inconclusive or had unknown outcomes.

Exhibit 2.7: Selected Law Enforcement Uses of Driver's License Data

Selected Uses of Driver's License Data Described by Law Enforcement Representatives	Appropriate	Not Appropriate
Records clerk uses driver's license information to confirm, correct, or complete work done by others, or to complete information in the Computer Aided Dispatch system.	✓	
Records clerk looks at photograph to complete missing race information.		✓
Records clerk looks at driver's license information to confirm or complete height information when entering information into the Statewide Supervision System.	✓	
Law enforcement supervisor looks at photograph to put a face with a name when reviewing initial complaint reports or arrest reports.		✓
Personnel use driver's license data if someone who is applying for a gun permit does not have a photo ID.		✓
The property clerk might use driver's license data in order to return property to someone who does not have his or her ID.		✓
Personnel use driver's license data to find person to contact for a death notification.	✓	
Officer uses driver's license photographs to put a face with a name in a tip, complaint, threat, or warrant.	✓	
Officer uses driver's license data to confirm the identity and license status of a person who is driving without a license.	✓	
Investigator uses driver's license photographs to confirm identities of individuals involved in an investigation.	✓	
On patrol, officers run a license plate and the driver's license information of the registered owner.	✓	
Officer runs information of law enforcement personnel in neighboring or collaborating jurisdictions to see who they are.		✓

NOTE: We assessed appropriateness with reference to permissible uses in state and federal law and in consultation with Driver and Vehicle Services Division staff.

SOURCES: Office of the Legislative Auditor and group discussions and site visits with representatives of law enforcement agencies.

Our analyses of queries to the DVS Web site identified many law enforcement users who possibly engaged in inappropriate query activity at least once during fiscal year 2012. It is important to note that activity that looks suspicious on its surface might reflect legitimate law enforcement uses. In addition, users did not have to perform a large number of queries to be identified as engaging in possibly inappropriate activity; some of the measures we used required that only one query meet our criteria for "questionable use."

Still, as Exhibit 2.8 shows, over one-third of law enforcement users accessed the driver's license information of someone with the same first and last name as theirs during fiscal year 2012, and around one-quarter accessed records of persons with the user's surname to a greater extent than one would expect by chance.[24] These users may have looked up their own or family members' information for non-work-related purposes.[25] Accessing driver's license information for non-work purposes is impermissible, even if it is not done maliciously. Failing to maintain clear boundaries about what uses are permissible could lead to more misuse.

[24] We counted a user if his or her queries of persons with the user's surname, as a proportion of all the user's queries, greatly exceeded the proportion one would expect by chance.

[25] As we indicate in the text, these uses that look questionable may have been for work purposes. For example, a dispatcher may have needed to look up a record of someone who, by chance, had the same first and last name as the dispatcher.

Exhibit 2.8: Law Enforcement Users Performing Questionable Queries through the DVS Web Site, Fiscal Year 2012

	Percentage of Law Enforcement Web-Site Users
Users who performed same-name queries	36%
Users who performed same-surname queries	25
Users whose queries of individuals of one sex were unusually high for at least one month[a]	9
Users with any of these questionable uses	53%

NOTES: There were 11,133 law enforcement users of the DVS Web site in fiscal year 2012. We truncated percentages (instead of rounding them) so as not to overstate the number of users who met the criteria for questionable queries. Queries that met our criteria may have been undertaken for legitimate law enforcement purposes.

[a] We counted only users whose percentage of queries of one sex in one month exceeded all users' queries for that sex for the full year by 25 percentage points or more. For example, women made up 44 percent of all records accessed during the year; we counted only the roughly 600 users for which women made up 69 percent (or more) of their queries in a month, and counted only months with at least 50 queries.

SOURCE: Office of the Legislative Auditor, analysis of Driver and Vehicle Services Division audit trail data.

We estimated that over half of the law enforcement users of the DVS Web site may have used it to perform questionable queries in fiscal year 2012, but not all of these users performed many of them.

More than 9 percent of law enforcement users of the DVS Web site conducted queries such that their percentage of records accessed for persons of one sex was unusually high for at least one month during fiscal year 2012. For example, women made up 44 percent of records accessed by law enforcement users overall, but women made up 69 percent (or more) of records accessed in a month by over 600 users.[26] There might be legitimate reasons that a user would access records of one sex disproportionately in a particular month. Still, such activity warrants further examination.

Finally, we could not discern a legitimate reason behind the queries of some "highly queried" individuals.[27] For example, the driver's license information of a murder victim was queried a total of 158 times in a single month by 110 users in 59 agencies. Law enforcement users queried some individuals' information more often during the first eight months of 2011 than they did following a far-reaching DVS inquiry into possible misuse. These individuals may have been suspects or criminals whose apprehension resulted in diminished interest, but the identities of two of them suggest reined-in curiosity as a more likely explanation. For some individuals, while we could not determine whether all of the queries were necessary, there seemed to be legitimate reasons for law enforcement interest.

[26] We counted only those months in which the user had at least 50 queries. Men made up about 56 percent of queries overall, but 81 percent or more of queries in a month by around 520 users.

[27] We identified approximately 450 individuals whom law enforcement users queried at least 100 times between January 2011 and June 2012. For a sample of 67, we used Internet searches to determine possible explanations for why they might have generated such law enforcement interest.

For example, some individuals were suspects in crimes around the time of the queries. Other individuals had had repeated contacts with law enforcement, perhaps explaining the interest.

TRAINING AND ACCESS

The Department of Public Safety (DPS) has made training available to law enforcement users of driver's license information.

We identified practices for preventing inappropriate access to and use of sensitive data by reviewing documents published by organizations with knowledge about or experience with these responsibilities.[28] Below, we evaluate DPS's training and access policies and procedures against these practices.

Training Users

Generally accepted practices for training individuals who will have access to private or confidential data include requiring training that covers general security policies and appropriate use, providing refresher training, keeping training up to date, and maintaining training and test records. We found:

- **The Department of Public Safety does not have adequate training policies for all law enforcement users of driver's license data, and until recently, training content was incomplete.**

As Exhibit 2.9 shows, DPS has not required training of all law enforcement users who access driver's license information through the DVS Web site. Sworn officers are not required to take training. In contrast, civilian users must take training, as well as submit a signed agreement to DVS that attests to having done so. In the past, the training required of civilian law enforcement employees addressed general security policies, classification of data, and appropriate uses. It also discussed possible consequences for misuse, including suspension of DVS access or criminal charges. Until recently, however, the training did not address the fact that permissible uses of driver's license photographs are more limited than other driver's license data and did not include post-training tests of knowledge. New training, which DVS made available to law enforcement in January 2013, includes specific information about the uses of driver's license photographs and tests of knowledge.[29]

[28] We reviewed publications by the National Institute of Standards and Technology (special publications 800-14, 800-53, 800-61, 800-92, and 800-122); the Office of Management and Budget (Memorandum 06-16, Memorandum 07-16, and Circular A-130); the U.S. Department of Justice (*Privacy, Civil Rights, and Civil Liberties Policy Development Guide: For State, Local, and Tribal Justice Entities* and *The National Criminal Intelligence Sharing Plan*); and the Federal Bureau of Investigation (*Criminal Justice Information Services (CJIS) Security Policy, Version 5.0* and *National Crime Information Center (NCIC) 2000 Operating Manual*). We also reviewed sections of the *U.S. Code* and the *Code of Federal Regulations*, as well as the Minnesota Board of Peace Officer Standards and Training Administrative Manual.

[29] DVS staff have indicated that this new training will be required for civilian law enforcement staff in place of the old training.

In January 2013, DVS released improved training for law enforcement users, but DVS does not require all those users to take its training.

Exhibit 2.9: Training Policies for Law Enforcement Users of the DVS Web Site Compared to Generally Accepted Practices, December 2012

Accepted Practice[a]	Training requirements for: Civilian Employees	Sworn Officers
Train all users in policies regarding general security	Yes	No
Train all users in appropriate use of data	Yes	No
Provide refresher training	No[b]	NA
Keep training up to date	Yes	NA
Maintain training and test records	Mixed/NA[c]	NA

NOTES: Table reflects requirements by the Driver and Vehicle Services Division of the Department of Public Safety. Law enforcement agencies employing users of the DVS Web site could have additional training requirements. "NA" means "not applicable;" DVS does not require training of sworn officers.

[a] Office of the Legislative Auditor staff developed a list of best, recommended, or generally accepted practices related to sensitive data. Referenced materials included publications by: the National Institute of Standards and Technology (special publications 800-14, 800-53, 800-61, 800-92, and 800-122); the Office of Management and Budget (Memorandum 06-16, Memorandum 07-16, and Circular A-130); the U.S. Department of Justice (*Privacy, Civil Rights, and Civil Liberties Policy Development Guide: For State, Local, and Tribal Justice Entities* and *The National Criminal Intelligence Sharing Plan*); the Federal Bureau of Investigation (*Criminal Justice Information Services (CJIS) Security Policy, Version 5.0* and *National Crime Information Center (NCIC) 2000 Operating Manual*). Staff also reviewed sections of *U.S. Code* and the *Code of Federal Regulations*, as well as the Minnesota Board of Peace Officer Standards and Training Administrative Manual.

[b] DVS does not provide refresher training, but individuals can retake the training DVS offers.

[c] DVS does not have an independent way to document that users have taken training. It requires civilian employees to sign a user agreement that, among other things, attests to the employee having taken training. DVS keeps these agreements. DVS training did not require tests of knowledge until January 2013.

SOURCE: Office of the Legislative Auditor.

Training policies for users who access driver's license information using BCA systems are generally consistent with accepted practices, but the policies are not specific to driver's license data. Rather, the policies reflect BCA's responsibility to administer the state's secure criminal justice network.[30] Through online and classroom options, training covers overall system security and, in general, access to and use and dissemination of data accessed through the network. Training also covers inappropriate use and mentions possible consequences of misuse. Training stresses that BCA systems are "for criminal justice purposes only," but provides little guidance specific to driver's license data.[31] As a result, individuals could finish training with the understanding that all driver's license information

[30] As discussed in Chapter 1, BCA systems provide access to driver's license data through the state's secure Criminal Justice Data Communications Network, also known as the CJDN. The Federal Bureau of Investigation has training requirements that agencies that administer secure criminal justice networks must meet.

[31] During BCA's biennial conference for criminal justice data users held in September 2012, two sessions focused on appropriate use of driver's license data. We did not consider these sessions to be part of BCA's standard training.

accessed through the network is available for any criminal justice purpose, when permissible uses of driver's license photographs are more limited than that.

Controlling Access

Exhibit 2.10 lists generally accepted practices for controlling access to data. Some practices that DPS does not use may not be practical given the nature of law enforcement. For example, restricting access to certain times of the day or days of the week could impinge upon the ability of law enforcement personnel to do their jobs.[32] Focusing on the other practices, we found:

- **Although the Department of Public Safety has several good practices for managing access to driver's license data, its implementation of some practices allows opportunity for misuse.**

DPS and law enforcement agencies share responsibility for managing access to driver's license information.

DPS uses several accepted practices to manage law enforcement access to driver's license data, whether the access occurs through the DVS Web site or BCA systems.[33] For example, both DVS and BCA specify access privileges, disable user accounts after persons leave employment, and require strong passwords.[34] In addition, users of the DVS Web site or BCA's Law Enforcement Message Switch or Integrated Search Service are greeted by a log-in screen that tells them that their activity may be monitored and misuse could result in consequences.[35]

The department has not implemented some practices well, however. The process for disabling user accounts of people who no longer need access to the DVS Web site is sometimes ineffective, allowing persons to gain access with invalid credentials. Until July 2012, this deficiency was made worse by DVS allowing accounts to remain dormant for 500 days before inactivating them. Now the division inactivates dormant accounts after 120 days.

[32] DVS has implemented some such restrictions for non-law-enforcement users of the Web site.

[33] As with training practices discussed above, the practices used for access to the BCA systems are for access to data through the Criminal Justice Data Communications Network and are not specific to driver's license data.

[34] BCA delegates responsibility for some of these practices to law enforcement agency staff. For example, a "Terminal Agency Coordinator" at each agency is responsible for assigning staff to groups in the Law Enforcement Message Switch, and that assignment determines the level of access. The coordinator is also responsible for disabling that access when a user leaves employment.

[35] Law enforcement agencies can access data through the Law Enforcement Message Switch using a BCA-provided interface or one provided by another vendor, such as the provider of their records management system. The log-in screens for BCA-provided interfaces include information about monitoring and consequences for misuse. According to BCA staff, users in most law enforcement agencies would not see a warning screen for access via mobile devices.

Exhibit 2.10: Generally Accepted Practices for Managing Access to Not Public Data

- Require signed user agreements
- Assign each user a unique identifier
- Specify users' access rights and privileges
- Disable user identifications after periods of inactivity and when a person leaves employment
- Require strong passwords
- Limit or disable remote and wireless access
- Lock user accounts after a certain number of failed login attempts
- Employ time-of-day or day-of-week restrictions
- Display notice on log-in screen warning that actions may be monitored and summarizing penalties

NOTE: Office of the Legislative Auditor staff developed a list of best, recommended, or generally accepted practices related to sensitive data. Referenced materials included publications by: the National Institute of Standards and Technology (special publications 800-14, 800-53, 800-61, 800-92, and 800-122); the Office of Management and Budget (Memorandum 06-16, Memorandum 07-16, and Circular A-130); the U.S. Department of Justice (*Privacy, Civil Rights, and Civil Liberties Policy Development Guide: For State, Local, and Tribal Justice Entities* and *The National Criminal Intelligence Sharing Plan*); the Federal Bureau of Investigation (*Criminal Justice Information Services (CJIS) Security Policy, Version 5.0* and *National Crime Information Center (NCIC) 2000 Operating Manual*). Staff also reviewed sections of *U.S. Code* and the *Code of Federal Regulations*, as well as the Minnesota Board of Peace Officer Standards and Training Administrative Manual.

SOURCE: Office of the Legislative Auditor.

Some practices for managing access to sensitive data may not be practical for law enforcement users.

DVS's approach to providing access to historical driver's license photographs is too permissive.

In addition, DVS is exercising insufficient control over driver's license photographs. First, although the division specifies user privileges, users who are granted access to driver's license photographs through the DVS Web site have access to all photographs, not just current ones. Second, during our evaluation, DVS learned that a local records management system used by some agencies automatically stored a copy of a person's current driver's license photograph with incident records.[36] This practice seems inconsistent with statutory language limiting the permissible uses of driver's license photographs.[37] Finally, it is possible to save a copy of a driver's license photograph accessed through the DVS Web site or BCA systems to a computer hard drive. Since authorized users can access the DVS Web site from any computer with Internet access, this means they could save photographs to non-work computers.[38]

DPS has not implemented other access management practices for all users. For example, DPS does not require a user agreement for sworn officers with access to the DVS Web site. Civilian law enforcement employees must sign a user agreement justifying their need for driver's license information, including their

[36] According to DVS staff, they had a conversation with the vendor to explain that this is not permissible.

[37] *Minnesota Statutes* 2012, 13.05, subd. 3; and 171.07, subd. 1a.

[38] According to BCA staff, it would be extremely difficult for users to access BCA systems from a non-work computer, but users could save photographs to a work computer and transfer them to a non-work computer via a portable storage device.

specific needs for access to driver's license photographs.[39] DVS staff review the agreements before granting access. BCA has a signed intra-agency agreement with DVS.[40] Agencies with employees who access BCA systems sign an agreement taking responsibility for access by their staff, among other things. Thus, it is only sworn officers who use the DVS Web site for whom DPS does not require an agreement, signed by the user or his or her employer, taking responsibility for appropriate access.

DPS does not require signed user agreements for sworn officers who use the DVS Web site.

Other access management practices vary by means of access. For example, DPS requires individual identification of DVS Web site users and users of some BCA systems, but does not require it for access to BCA systems through mobile devices. That is, users can log in to a mobile computer and access data without BCA knowing their identity.[41] In addition, according to staff, users of the DVS Web site or BCA's Integrated Search Service are locked out of those systems after a certain number of failed log-in attempts, but that is not the case with users of the Law Enforcement Message Switch. Finally, DPS does not limit remote and wireless access to the DVS Web site. Authorized users can access the Web site using any computer with Internet access. In contrast, access to BCA systems is restricted to devices with access to the state's secure criminal justice data network.

Recommendations

DPS has some good training and access practices, but others need attention. A challenge for the department is that, while the department has the data, the law enforcement users are employed by hundreds of state and local law enforcement agencies. Law enforcement agencies are responsible for seeing that their employees are sufficiently trained and determining who needs access to information to do their work. We direct the following recommendations primarily to DPS, but it will need to work with law enforcement agencies individually or through their associations to accomplish some of them. We also make one recommendation for consideration by chief law enforcement officers.

DPS and chief law enforcement officers will need to work together more diligently to ensure users of driver's license data are sufficiently trained and have appropriate access to data.

There are two ongoing initiatives that might influence the implementation of our recommendations. First, the department is developing a new system to provide access to information through DVS. Extensive modifications to the existing system might not be wise investments. Second, the department is considering providing driver's license information to law enforcement through BCA systems only. Depending on whether and how DPS moves forward with this, our recommendation targeting DVS access practices is less important for law

[39] One law enforcement agency has determined that its dispatchers and some support staff no longer need access to driver's license photographs through the DVS Web site.

[40] The agreement specifies the purposes for which BCA will use the data and assigns to BCA the "responsibility for providing adequate supervision and training to its employees to ensure compliance with the Data Practices Act and all applicable state and federal laws."

[41] According to BCA staff, each user is associated with a unique identifier except for queries from mobile devices. Although BCA does not know the identity of the individual accessing the data, agencies must control access to mobile devices and keep records of their users' transactions as required by the Federal Bureau of Investigation.

enforcement users, but may still be relevant to other users. Regardless of how these two initiatives progress, the training issues we identified need attention.

RECOMMENDATIONS

To increase awareness of permissible uses of driver's license data:

- ***The Department of Public Safety (DPS) should find additional ways to make information about permissible uses available;***
- ***Chief law enforcement officers should consider requiring their employees who use driver's license data to take training on the topic; and***
- ***DPS should work with the Sheriffs' Association and Chiefs of Police Association to develop a model policy for driver's license data use.***

DPS and chief law enforcement officers need to firmly establish expectations for appropriate use of driver's license data by law enforcement personnel.

It is important that DPS and law enforcement agencies provide clear and consistent information to law enforcement users of driver's license data in order to have a reasonable expectation that users will access and use the data appropriately. Minnesota used to treat driver's license information as public. In addition, some law enforcement representatives said that when DVS first made driver's license information available through the Web site, the classification of the data and their permissible uses were not emphasized. These factors, along with misuse that has occurred, suggest that an effort to firmly establish the appropriate uses of driver's license data and the DVS Web site is warranted. The training DPS released in January, along with additional sources of information and a model policy, could lay the foundation for responsible use.

First, DPS should develop additional ways of providing law enforcement users with information about appropriate uses of driver's license information. For example, it could create a periodic bulletin summarizing misuse identified during investigations. The bulletin could be sent to law enforcement agencies and posted on the DPS Web site to provide the public with information about monitoring efforts and investigative findings. DPS should also develop a short document focused on appropriate uses of driver's license data by criminal justice agencies; BCA could include the document in the resources it provides during basic training of users of the Criminal Justice Data Communications Network. Finally, BCA could include the DVS training on its Web site for persons who access driver's license information through BCA systems. According to BCA staff, they are planning to require users who want to access DVS data through the Integrated Search Service to complete DVS training first.

Second, chief law enforcement officers should consider requiring all users of driver's license information, regardless of how they access it, to complete the DVS training. While we think efficiency and consistency are served by DPS developing training on appropriate use, we think employers should be responsible for making sure their employees take it. The training concludes with

a certificate that individuals can print for their supervisor to sign and include in their personnel file.

Finally, a model policy is a complementary approach to training. A joint effort by DPS and law enforcement associations could create a comprehensive and accurate policy that is clear and relevant to law enforcement personnel. The policy should attempt to clarify appropriate uses of driver's license data, clearly articulate the limited uses of driver's license photographs, and outline possible consequences for inappropriate use.

Some law enforcement representatives said their agencies already had policies that covered driver's license information use, either specifically or under broad policies. Some representatives did not think a model policy was necessary, while others said they would welcome one. We think that, along with requiring training, a model policy will show agencies' due diligence to inform users about appropriate use and the gravity of misuse.

Not all law enforcement representatives with whom we spoke thought a uniform policy for driver's license data was needed.

One concern we heard about a model policy for driver's license data is that law enforcement personnel use many sources of private data. Some law enforcement representatives thought a policy that encompasses all not public data, not just driver's license data, would be better. The group that develops the policy can determine whether a single policy covering not public data is feasible. On the one hand, such a policy might emphasize the importance of data classification and reduce some of the confusion that surrounds it. On the other hand, it could be difficult to clarify the limited permissible uses of certain data in a comprehensive policy.

RECOMMENDATION

The Department of Public Safety should strengthen controls over law enforcement users' access to driver's license information.

It is important that government agencies protect private data from access that is inconsistent with the data's permissible uses. Above, we identified several practices that are lacking altogether or in their execution. The Department of Public Safety should work with law enforcement representatives to determine the best ways to achieve better access controls given information needs and technological considerations. Because the DVS Web site is available to authorized users through any computer with Internet access, it is particularly important that DPS address issues related to the Web site. We have listed three areas that we think need attention related to DVS Web site access.

DVS and law enforcement agencies need to make sure user accounts are disabled when persons leave employment, change to work assignments that do not require Web site access, or go on long-term leave. Law enforcement agencies need to alert DVS when such changes occur. DVS can assist with the task by sending chief law enforcement officers, periodically and upon request, a list of their employees who have Web-site access. Division staff work with law enforcement agencies to do some checking already, such as when a new contact person is

named at an agency. We suggest the addition of routine checks that are independent of other events.

DPS should consider requiring law enforcement agencies to sign a user agreement for their personnel to access the DVS Web site.[42] There is currently no documented assignment or acceptance of responsibility for sworn law enforcement officers who access the DVS Web site. Such an agreement could draw from the intra-agency agreement BCA signs for DVS data or the agreement that law enforcement agencies sign for access to BCA systems. An agreement could clarify law enforcement agencies' responsibilities to (1) request access only for those who need it and only to the information they need, (2) inform DVS when someone no longer needs access, and (3) observe the data classification of driver's license data. In addition, an agreement could clarify agencies' responsibility to train their employees, inform agencies that DVS collects and monitors data about employees' use of the DVS Web site, and clarify agencies' obligation to cooperate with investigations into possible misuse of the Web site.

DPS should work with law enforcement agencies to improve control over access to the DVS Web site.

Finally, DPS should consider modifying how it grants access to historical driver's license photographs. Currently, the DVS database does not separate current from historical photographs. When a user is granted access to photographs through the DVS Web site, the user receives access to all photographs. Many of the law enforcement uses of driver's license photographs that we heard about require current photographs for identity confirmation. The uses of historical photographs were less numerous. As DVS designs the new driver's license and vehicle registration data system, it should confer with law enforcement representatives about whether access to historical photographs could be granted more selectively to strengthen privacy protections while still meeting public safety needs.

INQUIRIES AND INVESTIGATIONS

Consistent with generally accepted practices, DVS and BCA each record queries of driver's license information in audit trails. An audit trail logs a user's identifier, the employing agency, what information was queried, and when.[43] The DVS audit trail also includes the name of the person whose username and password are associated with the query and the Internet Protocol address from which the query originated. DVS retains audit trail data indefinitely, while BCA retains them for at least six years. We found, however, that:

- **Neither DVS nor BCA does much proactive monitoring of law enforcement agencies' use of driver's license information.**

According to DPS officials, limited resources assigned to monitor audit trail activity prevent DVS and BCA from doing more proactive work to identify inappropriate use of driver's license information. DVS staff said that most of the

[42] Chief law enforcement officers have the option of requiring signed individual user agreements from their sworn officers.

[43] For queries through BCA systems using a mobile device, the audit log includes a device identifier rather than a user identifier.

division's use of the audit trail is reactive, partly because of staffing levels and the current information system's lack of sophistication. DVS assigns less than one full-time-equivalent person to audit-related work. BCA does not conduct proactive audits of driver's license data use. Its audit resources are focused on audits required by state and federal law, which do not include audits of driver's license activity. According to BCA staff, the division has purchased pattern analytics software to be more proactive about catching misuse, but this effort is still in development.

DVS and BCA use their audit trails to respond to inquiries from employers and other individuals about use of driver's license information. DVS does some proactive work, as well, to identify possible misuse. In this section, we describe DVS and BCA inquiries into use of driver's license information. We also discuss law enforcement agencies' investigations of alleged misuse and consequences and sanctions for misuse.

DVS and BCA each maintain a record of law enforcement users' access to driver's license information.

Employer Inquiries

Chief law enforcement officers can request audit trail information from DVS, BCA, or both. Requests might be instigated by citizen complaints or suspicious behavior identified internally. Agencies may also request information as part of a broad internal affairs investigation into an employee's work rather than due solely to concerns about his or her use of driver's license information. In some cases, agencies have requested DVS audit trail information for routine monitoring. For example, one sheriff's office requested DVS audit trail information for all dispatchers for a 60-day period. DVS and BCA respond to employer requests by providing the requested information. As Exhibit 2.11 shows, DVS responded to employer inquiries from 31 law enforcement agencies in fiscal year 2012.

Individual Inquiries

Both DVS and BCA respond to requests from individuals about access to their driver's license information. However, we found:

- **Until recently, the Department of Public Safety did not have a consistent approach for handling individuals' requests for information about queries of their driver's license data.**

BCA and DVS classify their audit trail data differently and, prior to October 2012, responded differently to requests from individuals. Based on a security declaration by the Commissioner of Public Safety, BCA considers the audit trail data to be private data about the person whose information was searched.[44] It requires requests in writing and, after verifying the person's identity, provides the

[44] The Commissioner of Public Safety has declared that all audit trail data related to the state's Criminal Justice Data Communications Network are "security information," making them private or nonpublic. See Commissioner Ramona L. Dohman, "Determination of Classification of Data at BCA/MNJIS Division and Authorization for the Sharing of That Data," March 11, 2011.

individual with his or her private data.[45] The individual can follow up with law enforcement agencies if he or she is concerned about any use. BCA staff said the bureau does not receive many requests from individuals who are concerned about who has accessed their driver's license information.

Exhibit 2.11: Law Enforcement Agencies Involved in Inquiries of DVS Web Site Use, Fiscal Year 2012

Inquiries about use of DVS's Web site are initiated in various ways.

	Agencies
Law enforcement agency request	31
Individual inquiry to DVS[a]	26
DVS expanded inquiries[b]	25
DVS "Top 50" monitoring[c]	5
DVS review of ex-employee use[d]	1
Unduplicated count	69

NOTES: There were approximately 435 law enforcement agencies in Minnesota in 2012. DVS did not contact all agencies involved in inquiries to request investigation.

[a] This category includes agencies specifically named by an individual making an inquiry. If the individual did not name specific agencies, the figure includes agencies with employees who queried the individual's name.

[b] This category reflects agencies to which DVS expanded inquiries after an individual or a law enforcement agency made an inquiry that was limited in scope.

[c] These agencies had employees appear on a "Top 50" list of Web site users.

[d] This review involved an agency that did not inform DVS promptly of some employees' termination.

SOURCE: Office of the Legislative Auditor, review of Driver and Vehicle Services Division audit files.

DVS and BCA have handled individual inquiries about use of driver's license data differently, and DVS's approach has been evolving.

In contrast, prior to October 2012, DVS considered all of the audit trail data to be electronic access data that record users' activity, with the user (rather than the person whose information was searched) being the data subject.[46] DVS required individuals to submit concerns in writing articulating the basis of their concern. If staff considered a person's concerns reasonable, they reviewed all queries of the person's information and asked employing agencies to investigate any unusual query activity by their users. Exhibit 2.11 shows DVS reviewed activity involving 26 law enforcement agencies involved in individuals' complaints.[47]

In October 2012, DVS changed its response to individual inquiries. The division still considers user information in the audit trail to be electronic access data, but now provides to persons who were searched the name of the employing agency and date, time, and type of query. DVS staff provide an individual with that

[45] The information provided by BCA does not include the name of the person who searched for the citizen's data.

[46] *Minnesota Statutes* 2012, 13.15, subd. 1(a), defines electronic access data, in part, as "data created, collected, or maintained about a person's access to a government entity's computer."

[47] This figure includes agencies specifically named by an individual making an inquiry. If the individual did not name specific agencies, the figure includes agencies with employees who queried the individual's name.

information upon receiving a written request, but do not verify the individual's identity before doing so.[48] Staff still follow up with employing agencies about unusual query activity.

Expanded Inquiries and Proactive Monitoring

DPS uses its audit trails to look for possible misuse in a few ways. First, DVS expands reviews based on individuals' inquiries, and both DVS and BCA expand reviews based on agency inquiries. For example, if a woman has concerns that personnel in a specific law enforcement agency accessed her information inappropriately, DVS staff review all recorded queries of the woman's information. The audit trail might show queries by employees from multiple agencies. In that case, DVS staff might ask each agency to investigate. Second, at times, DVS has reviewed a user's activity after learning from a law enforcement agency about the user's termination from employment. As Exhibit 2.11 shows, in fiscal year 2012, DVS expanded reviews based on narrow citizen complaints or agency requests to 25 agencies and followed up with 1 agency after a review showed a former employee continued to use the Web site after his last day of work.

Since 2010, DVS has generated monthly lists to identify possible misuse of its Web site.

Third, since 2010, DVS has generated monthly lists to identify possible targets for investigation. These monthly lists are not specific to law enforcement use, but can include law enforcement users. For example, there is a list of the top 50 searchers of driver's license photographs and a list of the top 50 searchers of driver's license demographic data. More recently, DVS started identifying the top 25 persons searched as another proactive monitoring tool. One user identified through a top-50 list had looked up close to 200 individuals for non-work-related purposes during a one-month period. Still, we found:

- **DVS's proactive monitoring reports may be inefficient tools for identifying inappropriate law enforcement use.**

First, as mentioned above, the lists are not restricted to law enforcement users. Second, they have historically focused on high-volume use, not suspicious use; the more recent top-25 report might identify some users with unremarkable query volume but suspicious uses. Third, staff have not established baselines for reasonable levels of activity for individuals based on job assignments, size of jurisdiction, and other factors that could affect query volume. Lastly, as we discovered in our own analysis of frequently queried individuals, attempting to determine who the people are and why they might be under law enforcement scrutiny is time consuming and not always informative.

Investigations of Possible Misuse

Law enforcement agencies are responsible for investigating possible misuse of driver's license information by their personnel. Investigations are necessary to

[48] The request must include the individual's name, date of birth, and driver's license number. If the request pertains to the activity of a single user, staff provide information about all of the queries from that user's agency.

identify and correct impermissible uses, and law enforcement agencies are in the best position to assess the activities of their staff. However, we found that:

- **The Department of Public Safety does not always receive conclusive and accurate information from law enforcement agencies about their investigations into possible misuse of driver's license information.**

Information that law enforcement agencies provide to DPS about their investigations might reflect challenges in conducting investigations of possible misuse, lack of understanding among those investigating about what misuse includes, or lack of responsiveness.

Investigating an allegation that a person has misused driver's license data—a responsibility of the employing law enforcement agency—can be challenging.

Reaching conclusions about misuse of driver's license information can be challenging. To investigate possible misuse, supervisors might interview the user and check their local computer-aided dispatch system or records management system to see if the queries had legitimate work-related purposes. However, legitimate queries might not have local records associated with them. In addition, the passage of time may make interviews difficult. For example, DVS might ask a chief law enforcement officer to investigate a single query of a complainant's information transacted four years earlier. Asking an officer about an isolated query, especially one from the distant past, may not be fruitful. According to a response to DVS from one agency, that agency does not investigate complaints after one year has passed unless there is an allegation of a crime or personal gain.

In addition, some investigating officers might not know the full range of activities that constitute inappropriate use. For example, the inappropriate uses listed in Exhibit 2.7 might go unnoticed by investigators in agencies that use the information in those ways. During our file reviews, we noted two investigations that concluded with a finding of no misuse, although the users appeared to have accessed their own information. Querying one's own information may not raise concerns that other forms of misuse do, but it is still misuse.

In addition, it appears that chief law enforcement officers are not equally responsive to notifications of possible misuse of driver's license information and requests for information about the outcome of misuse investigations. For example, DVS sent two agencies notice that a staff person was among the "top 50" users in one month. One chief law enforcement officer requested a copy of the person's audit trail for the month and found inappropriate use. The other officer responded that the volume of use was reasonable given the user's job duties, apparently without requesting an audit trail. DVS did not record conclusions for some fiscal year 2012 investigations because agencies did not respond to DVS's requests for the outcome. We do not know if these agencies did not do investigations or simply did not provide DVS with the results. BCA staff also indicated that agencies often do not inform BCA of the outcome of investigations.

Consequences for Misuse

If a person is found to have misused driver's license data, sanctions may be imposed by DPS, the user's employer, or both. The user could also face criminal charges or be named in a civil suit.[49] However, we found:

- **Neither BCA nor DVS has a written policy for applying sanctions against individuals who misuse driver's license information.**

According to DVS staff, they determine consequences for misuse based on the extent of misuse and precedent from similar past violations. DVS may take no action or may impose sanctions that range from a warning letter to indefinite or permanent suspension of access to the Web site. Exhibit 2.12 summarizes consequences issued by DVS as a result of fiscal year 2012 investigations into misuse of the Web site. BCA staff indicated that they rely on law enforcement agencies to impose sanctions because it is very difficult to disable a single user's access to driver's license data without also disabling the user's access to other data sources. BCA records show the bureau sanctioned one of the six individuals who misused DVS data through the BCA systems.[50] This user's repeated misuse resulted in permanent revocation of access to the Criminal Justice Data Communications Network.

Consequences that law enforcement agencies impose for misuse of driver's license information can vary for several reasons.

According to state and local law enforcement agency representatives, employer consequences to individuals who similarly misuse access to driver's license information may differ and may not always reflect the supervisors' preferences. Law enforcement representatives with whom we spoke thought that imposing consequences for misuse is important. They noted, however, that individuals who misuse data might experience different consequences due to the chief law enforcement officer's philosophy, other issues about the employees' performance, the mediation and grievance process, and decisions by agencies whether to indemnify individuals in the event of a lawsuit. In addition, the effect of DPS sanctions might vary. For example, a large agency may be able to accommodate an employee's three-month suspension of DVS Web site access by moving the person to a different position, while a small agency without that flexibility might have to suspend or terminate the person's employment.

As Exhibit 2.12 shows, sanctions imposed by law enforcement agencies after investigations involving DVS Web site use ranged from counseling to termination.[51] Also, we are aware of one agency that asked DVS to increase the DVS sanctions for Web site misuse beyond what DVS intended; the agency asked DVS to suspend some users it otherwise would not have and lengthen the suspension for others. DVS obliged the agency's request. Employers of the six individuals found to have misused DVS information through BCA systems

[49] Various sections of Minnesota law—including *Minnesota Statutes* 2012, 13.09; 171.12, subd. 7(a); and 609.43 and 609.891—could provide a basis for criminal charges depending on the circumstances of misuse.

[50] As noted previously, misuse documented in DVS and BCA audit files may include inappropriate use of motor vehicle information, rather than driver's license information.

[51] Sanctions may have involved employee conduct issues other than misuse of the DVS Web site.

Law enforcement personnel who misuse the DVS Web site may be sanctioned by their employer and DVS.

Exhibit 2.12: Law Enforcement Employees Sanctioned for Misuse of the DVS Web Site, Fiscal Year 2012

	Employees Sanctioned[a]		
Driver and Vehicle Services Sanctions	**72**		
Letter		44	
Suspension		28	
15 days			8
1 month			6
3 months			9
6 months			3
12 months			1
Indefinite			1
Law Enforcement Agency Sanctions[b]	**36**		
Unspecified[c]		23	
Coaching or counseling		5	
Written warning or reprimand		5	
Termination		2	
Suspension		1	

NOTES: Eighty-eight law enforcement personnel were determined to have misused the DVS Web site. Table reflects law enforcement agency investigations in response to inquiries initiated in fiscal year 2012. There were 11,133 law enforcement users of the DVS Web site in Minnesota in fiscal year 2012.

[a] Employees may have been sanctioned by DVS and/or their employer. Count includes two former employees who continued to use their DVS Web site access.

[b] In addition to the employees sanctioned by their employer, two employees resigned.

[c] This category includes: "corrective action," "formally sanctioned," "coaching, counseling, and discipline," "addressed by police administration," "ranged from retraining to disciplinary actions," "will be addressed interdepartmentally," and "we are considering our options regarding disciplinary actions."

SOURCE: Office of the Legislative Auditor, review of Driver and Vehicle Services audit files.

sanctioned the users with retraining, oral reprimands, suspensions without pay, reassignment, or, in one case, possible termination.

Misuse of driver's license information can have consequences for agencies, too. First, state and local governments can face substantial financial consequences for employees' misuse. So far, a 2012 lawsuit filed under the Driver's Privacy Protection Act has resulted in settlements exceeding $1.0 million total.[52] Second, the law enforcement profession may suffer loss of credibility or esteem when some of its members behave irresponsibly.

[52] Anne Marie Rasmusson v. City of Bloomington, et al., No. 12-632 (D. Minn. filed March 12, 2012).

Recommendations

Increasing awareness about appropriate use and improving access controls may help minimize inappropriate use of driver's license information. Nevertheless, activities to monitor use need to be supported, and agencies and individuals need to be held accountable when misuse occurs.

RECOMMENDATION

Chief law enforcement officers should consider doing more proactive monitoring of their employees' use of driver's license data.

Chief law enforcement officers are in the best position to monitor their staff's use of driver's license information and respond to misuse.

We think chief law enforcement officers and other law enforcement agency supervisors should consider doing more proactive inquiries into their employees' use of driver's license information. Proactive monitoring takes resources, but agencies could limit the number and scope of reviews to make the work manageable. For example, a chief law enforcement officer could select two employees a month and request their DVS or BCA driver's license queries for a one-month period. DVS could assist by keeping chief law enforcement officers informed about what constitutes inappropriate use and patterns that might signify misuse.

Law enforcement supervisors need not investigate every query in an audit trail in order to monitor use. In our analysis of query data, we looked for users who appeared to access their own information, relatives' information, or information about members of one sex disproportionately. We also identified users who queried people in the news. Supervisors could look for similar activity, as well as whether a user has queried co-workers' information or performed queries that are inconsistent with the user's work schedule and work assignments.

RECOMMENDATION

The Department of Public Safety should consider investing additional resources to monitor use of driver's license data and formalizing its approach to handling inquiries into use of these data.

Increased monitoring of driver's license data use will require additional resources.

If law enforcement agencies respond positively to our recommendation for more proactive monitoring, DPS may need to increase staff resources to manage the activity. Unless it can develop more targeted tools, we do not recommend that DVS undertake additional proactive monitoring at this point. We think it could be more effectively done by chief law enforcement officers who are in a better position than state agency employees to identify unusual patterns of use among their staff.

DPS should consider investing in technology to assist with proactive monitoring of use through the new driver's license and vehicle registration information system. For example, perhaps the system could allow for more flexibility in the types of monitoring reports DVS staff can generate, or identify users or query

subjects with unusual search patterns or activity. As noted previously, BCA recently purchased software to monitor queries of driver's license information through its systems.

With the potential for additional inquiries and instances of identified misuse, it would be prudent for DPS to consider formalizing how it will respond to inquiries, its criteria for requesting investigations into possible misuse, its expectations for responses to its requests, and sanctions when agencies are not responsive or individuals are found to have misused driver's license data. Crafting a sound approach to monitor and correct misuse of driver's license data will be difficult. There are real challenges to identifying possible misuse that warrants investigation, including the absence of individual identifiers for mobile access to DVS data through BCA systems and the different patterns of legitimate use that individual users or agencies could exhibit. The passage of time is a challenge to investigating possible misuse, especially absent a pattern of questionable activity. And misuse, when it is found, can vary greatly, from work-related misuse, to isolated lapses in judgment, to numerous violations of the law. All of these considerations speak to the need for a flexible and evolving approach.

As part of this effort, DPS should continue refining its approach to handling inquiries from members of the public about law enforcement personnel's use of driver's license information. The two divisions that handle these requests have a more similar approach now than in the past, but there are still some differences. For example, DVS does not verify a person's identity before providing private information. In addition, the two divisions retain their audit trail data for different lengths of time, affecting the amount of data individuals can request and receive. The department could also consider identifying a single point of contact within the agency to direct and coordinate individuals' inquiries about who has accessed their driver's license information.

CONCLUDING REMARKS

In Chapter 1, we outlined policy interests relevant to law enforcement use of information, including public safety, civil liberties, transparency, and privacy. We also described how state law, the Department of Public Safety, and law enforcement agencies balance these interests. In these remarks, we bring together how the state has managed these interests for driver's license data. We concluded that:

- **Overall, the state's approach to managing law enforcement use of driver's license data is reasonable, but privacy and transparency need additional attention.**

The Legislature has balanced policy issues related to law enforcement use of driver's license information by focusing on data classification and permissible uses, leaving to DPS and law enforcement agencies the responsibility to manage access and use. We think this approach is reasonable. We observed a real public safety need for law enforcement personnel to have access to driver's license data. Patrol officers in particular needed to access information quickly and frequently.

DPS and law enforcement agencies can use mechanisms that are already available—training, access controls, monitoring, and consequences—to improve protection of driver's license data.

At the same time, it is important that law enforcement personnel use driver's license information only for permissible purposes and respect individual privacy. Unfortunately, we found inappropriate work-related and non-work-related uses of driver's license data, although we were unable to quantify their full extent.

Our recommendations reflect our belief that DPS, along with chief law enforcement officers and their associations, can take steps to strengthen mechanisms that are already in place. DPS has created training on the classification and permissible uses of driver's license information and maintains audit trails, but as currently implemented, these and other training and access provisions are insufficient and not always effective. Most of our recommendations are aimed at improving DPS's efforts, but chief law enforcement officers should also do their part by making sure their staff are trained, requesting access to information only for staff who need it, monitoring their employees' use, and imposing consequences when they identify misuse.

We resisted recommending more legislated restrictions or technical controls (such as indicating purpose codes for each search). Putting too many restrictions and controls in place could compromise the usefulness of these data. The exception is historical driver's license photographs. We think the public safety need for and use of these data are fundamentally different from the need for and uses of current driver's license information and thus recommended that access to these data be granted more selectively.

Finally, we think it is important that DPS and law enforcement agencies be transparent about misuse of driver's license information when it occurs. As part of reminding users about appropriate use, we recommended that DPS create a periodic bulletin summarizing identified misuse of driver's license information. Our expectation is that the bulletin would be public information. We also recommended that DPS consider formalizing its approach to handling inquiries about searches of driver's license data.

3 Comprehensive Incident-Based Reporting System

The Bureau of Criminal Apprehension (BCA) manages the Comprehensive Incident-Based Reporting System (CIBRS).

The Comprehensive Incident-Based Reporting System (CIBRS) is a database that facilitates information sharing among Minnesota law enforcement agencies. Managed by the Bureau of Criminal Apprehension (BCA) in the Department of Public Safety, CIBRS contains incident data contributed by Minnesota law enforcement agencies.[1] Participating Minnesota law enforcement agencies can search CIBRS for information that might help them solve crimes or locate people.

In this chapter, we first provide an overview of the CIBRS database: the agencies that contribute data to it; the characteristics, classification, and permissible uses of its data; and how law enforcement personnel have used it to find information. Next we discuss whether law enforcement employees have used CIBRS for unauthorized purposes. We then evaluate how well BCA's training, limits on access, and audit program have protected CIBRS from inappropriate access and use and provide recommendations to improve those efforts. We conclude with thoughts on how well CIBRS balances the policy interests discussed in Chapter 1.

THE CIBRS DATABASE

The Legislature authorized CIBRS to facilitate information sharing among law enforcement agencies.

The Legislature authorized CIBRS in 2005 to provide law enforcement agencies with a means of sharing information.[2] CIBRS was designed as a "pointer system" that refers users to agencies that might have useful information, rather than as a database that contains all that information. Below, we describe law enforcement agencies' participation in CIBRS and summarize the contents of CIBRS as of July 2012. We also outline CIBRS' data practices requirements and permissible uses, as well as the extent to which law enforcement professionals have searched the database.[3]

Participating Agencies

State statutes specify which law enforcement agencies may participate in CIBRS. As Exhibit 3.1 shows, these Minnesota agencies include municipal police

[1] "Incidents" can include records of anything that a law enforcement officer comes upon or to which the officer is called to respond.

[2] *Laws of Minnesota* 2005, chapter 163, sec. 81. The Legislature has amended the section of statute governing CIBRS several times since then, mostly to authorize additional participating agencies and more purposes for searching CIBRS.

[3] We obtained an extract of CIBRS data as they existed on July 26, 2012. The data include a complete history of searches performed in CIBRS.

Exhibit 3.1: Agencies Eligible to Participate in CIBRS

- Minnesota municipal police departments
- Minnesota county sheriff's offices
- Bureau of Criminal Apprehension
- Fugitive Apprehension Unit, Department of Corrections
- Enforcement Division, Department of Natural Resources
- Metropolitan Airports Police
- Minnesota State Patrol
- Metropolitan Transit Police
- University of Minnesota Police Department

SOURCE: Office of the Legislative Auditor, summary of *Minnesota Statutes* 2012, 299C.40, subd. 1(c).

Under state law, only Minnesota law enforcement agencies may access CIBRS data, and agency participation is voluntary.

departments, county sheriff's offices, and certain state law enforcement agencies like the Minnesota State Patrol.

An agency's decision to participate in CIBRS is entirely voluntary. Participating agencies can submit incident records to CIBRS, search records, or both. The agencies access CIBRS through the state's secure Criminal Justice Data Communications Network (CJDN), so agencies without direct CJDN connections can participate only by collaborating with an agency that has a direct connection.[4]

If a law enforcement agency chooses to submit incident records to CIBRS, it does so by sharing records from its records management system. As we described in Chapter 1, records management systems contain records of law enforcement actions and responses to requests for service. Agencies cannot submit some portions of their incident records, such as any text notes describing the incident in detail or whether persons are suspected gang members. Agencies retain "ownership" of their incident data in CIBRS and can edit or delete them at any time.

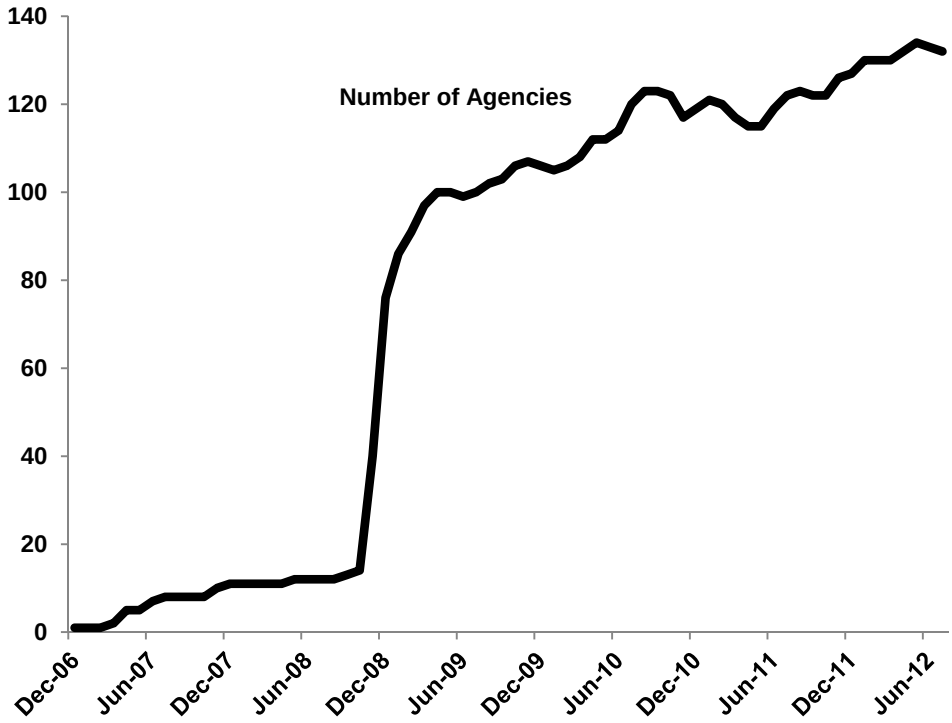
Since CIBRS' inception, 150 law enforcement agencies have had access to the system at some point. Exhibit 3.2 shows the growth in the number of agencies with CIBRS access since the first agency began participating in December 2006. In the last three months of 2008, 72 agencies gained access, but growth has been slower since then.

Several agencies appear to have ceased sharing information with CIBRS. As of July 2012, CIBRS contained no 2012 incident records from 33 agencies that had submitted records in earlier years. These agencies may have recorded no incidents that met their submission criteria, or they may have not submitted records for other reasons.

[4] BCA estimates that 100 small law enforcement agencies lack direct CJDN connections. All participating agencies, regardless of whether they have a direct connection or collaborate with another agency, must follow the same certification process before accessing CIBRS. We describe the certification process later in this chapter.

The number of agencies participating in CIBRS jumped in 2008 and has increased gradually since then.

Exhibit 3.2: Law Enforcement Agencies with CIBRS Access, December 2006 – July 2012



NOTES: Law enforcement agencies can participate in CIBRS by submitting data, searching data, or both. This chart shows the number of agencies that had access to CIBRS on the first day of each month. Not all agencies with access to CIBRS submit or search data.

SOURCE: Office of the Legislative Auditor, analysis of CIBRS data.

Incident Characteristics

In July 2012, CIBRS contained information about 2.86 million incidents contributed by 136 agencies. As Exhibit 3.3 shows, law enforcement agencies from the seven-county metropolitan area contributed the majority (73 percent) of these incidents. Among agencies outside the metropolitan area, those in the northeastern and southeastern parts of the state shared the most incidents. Slightly more than half of the agencies contributed fewer than 2,000 incidents each. Almost all incidents in CIBRS took place in or after 2000; about 55 percent of them occurred in or after 2008.

Exhibit 3.3: Geographic Coverage of CIBRS Incidents, July 2012

	Incidents	Percentage
Seven-County Metropolitan Area	**2,077,287**	**73%**
Outstate Areas	**785,900**	**27%**
Northeast	350,042	12
Southeast	238,605	8
East Central	101,916	4
Southwest	71,925	3
West Central	12,649	< 0.5
Northwest	10,763	< 0.5
Total	**2,863,187**	**100%**

NOTES: The seven-county metropolitan area includes incidents contributed by agencies in Anoka, Carver, Dakota, Hennepin, Ramsey, Scott, and Washington counties. "Outstate areas" includes incidents contributed by agencies in all counties outside the seven-county metropolitan area.

SOURCE: Office of the Legislative Auditor, analysis of CIBRS data.

Participating agencies may choose to submit only certain types of incidents or information to CIBRS.

Agencies can choose to submit only certain subsets of incidents to CIBRS. For example, some agencies do not submit misdemeanor traffic offenses. One agency we visited told us that it does not submit incidents to CIBRS until the incidents are no longer part of an active criminal investigation.[5] Another agency indicated that it submits only incidents for which investigators are seeking criminal charges.

Data submitted to CIBRS must fit into certain "data elements" established by BCA; Exhibit 3.4 displays a selection of them. Every incident record submitted to CIBRS must have certain administrative information, the data classification, and the incident date and time. Each CIBRS incident must also include at least one code indicating what kind of offense or offenses were committed as part of the incident.[6] As Exhibit 3.5 shows, most CIBRS incidents as of July 2012 contained a "miscellaneous" offense.[7] About 29 percent of CIBRS incidents included a property crime, while 8 percent included a crime against a person.[8]

[5] See the Appendix for a list of the law enforcement agencies we visited during the evaluation. According to *Minnesota Statutes* 2012, 13.82, subd. 7, a criminal investigation becomes inactive upon: "(a) a decision by the agency or appropriate prosecutorial authority not to pursue the case; (b) expiration of the time to bring a charge or file a complaint under the applicable statute of limitations, or 30 years after the commission of the offense, whichever comes earliest; or (c) exhaustion of or expiration of all rights of appeal by a person convicted on the basis of the investigative data."

[6] An incident can include multiple offenses, such as larceny and theft. Agencies use the Federal Bureau of Investigation (FBI) National Incident-Based Reporting System codes to classify offenses.

[7] While no further detail is available in CIBRS about these offenses, BCA staff said that they could include, for example, nuisance reports and traffic citations.

[8] These broad categories of offenses, such as crimes against persons, reflect the FBI groupings of National Incident-Based Reporting System offense codes.

Exhibit 3.4: Selected Information Agencies Can Submit to CIBRS

Incident Information

- Date and time[a]
- Location
- Data classification[a]
- Identifying number[a]
- Contributing agency identifier[a]

Offense Information

- Type (e.g., burglary or assault; incidents can include more than one offense)[a]
- Whether offense was completed or attempted

Person Information

- Role (arrestee, suspect, victim, witness, reporter, other)
- Name (a person's record can include more than one name, including nicknames)
- Address
- Age
- Physical description (gender, race, ethnicity, height, weight, eye color, hair color, build description)[b]
- Victim's relationship to alleged offender
- Date and time of arrest for persons arrested

Property Information

- Type (e.g., vehicle, drug, electronic device)
- Value
- Status (e.g., stolen, destroyed, recovered)
- Type and amount of drug(s)
- Make, model, license plate number, and color of vehicle(s)

NOTES: CIBRS has many data elements not included here. This table includes a selection of the most frequently submitted data elements according to BCA staff. Except as noted, incident records need not contain this information.

[a] Required information.

[b] CIBRS accepts height, weight, eye color, hair color, and build descriptions only for arrestees, suspects, and victims.

SOURCE: Office of the Legislative Auditor, summary of CIBRS documentation.

Agencies that submit data to CIBRS can submit a wide range of information.

Agencies can elect to submit other types of information for each incident. For example, they can share information about the people involved in the incident, such as alleged perpetrators, victims, witnesses, and persons who reported the incident. Among all CIBRS incidents, 93 percent contained information about at least one person; 34 percent contained information about a suspect, while just 8 percent contained witness information. Agencies may choose to submit information about some persons, but not others. For example, one agency we

Exhibit 3.5: Types of CIBRS Incidents, July 2012

Incidents Containing	Percentage of Incidents
Miscellaneous offense Includes offenses not otherwise classified below[a]	55%
Crime against property Includes burglary, theft, larceny, robbery, and various money-related offenses like fraud and embezzlement	29
Crime against society Includes loitering, disorderly conduct, drug offenses, gambling, pornography, prostitution, and weapons law violations	15
Crime against person Includes assault, homicide, abduction, and rape and other sex offenses	8
Other offense Includes non-criminal offenses (justifiable homicides, runaways)[b]	1

NOTES: N = 2,863,187 incidents in CIBRS as of July 26, 2012. We based this classification on BCA-provided groupings of National Incident-Based Reporting System offense codes. Percentages do not sum to 100 because incidents can include more than one type of offense.

[a] While no further detail is available in CIBRS about these offenses, BCA staff said that these could include, for example, nuisance reports and traffic citations.

[b] Three incidents that lacked an offense record for technical reasons are classified here as well.

SOURCE: Office of the Legislative Auditor, analysis of CIBRS data.

visited submits information only about suspects and arrestees. About one-third of the people in CIBRS in July 2012 were alleged perpetrators (suspects or arrestees). As Exhibit 3.6 shows, 18 percent of the people in CIBRS were suspects, and 17 percent were arrestees.[9]

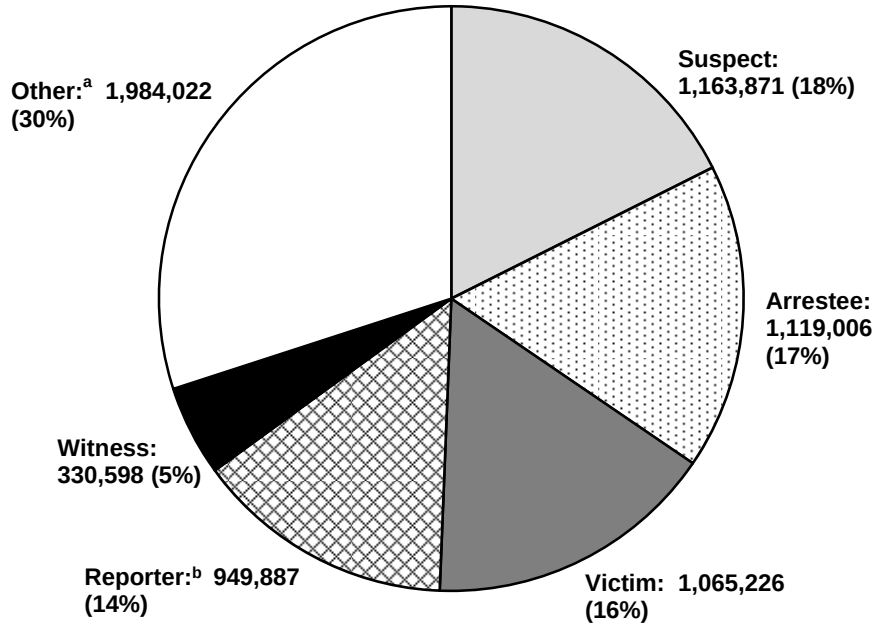
Agencies may also limit the personal information they submit. For instance, some agencies do not submit street names for people's addresses. Nevertheless, personal information is prevalent in CIBRS, as Exhibit 3.7 shows. For instance, 89 percent of people in CIBRS in July 2012 had both a first and a last name recorded. This varies by the role of the person in the incident, however. Only 53 percent of suspects had both a first and last name recorded in CIBRS. The vast majority of person records in the other role categories had a first and last name recorded.

Data Practices

Data practices include (1) data classification; (2) means by which individuals, including subjects of private data, can gain access to data; and (3) a process by which data subjects can challenge the accuracy or completeness of data about them.

[9] By "people in CIBRS," we do not mean the number of unique individuals in CIBRS. Unique individuals who are associated with multiple incidents appear multiple times in CIBRS. Because agencies may have recorded names, addresses, and other identifying information differently in different incidents, we do not know the number of individual people in CIBRS.

Exhibit 3.6: Roles of Persons in CIBRS Incidents, July 2012



Total person records: 6,612,610

NOTES: Figure reflects CIBRS data as of July 26, 2012, excluding approximately 15,000 person records that appear to be organizations. Unique individuals who are associated with multiple incidents appear multiple times in CIBRS. Because agencies may have recorded names, addresses, and other identifying information differently in different incidents, we do not know the number of individual people in CIBRS.

[a] Includes persons identified by agencies as "Complainant," "Driver," "Father," "Mother," "Passenger/Pedestrian," or "Other." Except for "Other," none of these is an official CIBRS category.

[b] Includes person(s) who reported the incident.

SOURCE: Office of the Legislative Auditor, analysis of CIBRS data.

In July 2012, over one-third of the people in CIBRS records were suspects or arrestees.

The Legislature has classified data in CIBRS as "not public."

State law classifies all data in CIBRS as not public.[10] The law classifies data that law enforcement agencies have not identified as part of an active criminal investigation as private or nonpublic. Under the law, data may be confidential or protected nonpublic if a law enforcement agency has identified them as part of an active criminal investigation. State law requires that confidential or protected nonpublic data in CIBRS become private or nonpublic if the agencies that contributed them do not confirm the confidential or protected nonpublic classification every 120 days. As of July 2012, about three-quarters of all CIBRS agencies had no confidential or protected nonpublic data in CIBRS.

[10] *Minnesota Statutes* 2012, 299C.40, subd. 4(b) and (c). Data in the originating agency retain their classification. In other words, public incident data remain public in the database of the agency that contributed the data, even though they are not public in CIBRS.

Exhibit 3.7: Personal Information in CIBRS, July 2012

Person's Role in Incident	Percentage of Person Records that Included: First and Last Name	Date of Birth	Street Name and City Name
Alleged perpetrator			
Arrestee	100%[a]	94%	80%
Suspect	53	46	38
Alleged victim	98	93	89
Other involved party			
Witness	99	74	74
Reporter	92	15	26
Other[b]	96	61	72
All CIBRS person records	89	63	63

NOTES: N = 6,612,610 person records in CIBRS as of July 26, 2012. This table excludes approximately 15,000 person records that appear to be organizations.

[a] More than 99.5 percent of arrestee records included a first and last name.

[b] Includes persons identified by agencies as "Complainant," "Driver," "Father," "Mother," "Passenger/Pedestrian," or "Other." Except for "Other," none of these is an official CIBRS category.

SOURCE: Office of the Legislative Auditor, analysis of CIBRS data.

Under the CIBRS section of statutes, data subjects may gain access to private CIBRS data about them, including the name of the agency that contributed the data.[11] They can also learn whether CIBRS contains any confidential information about them, though they cannot see that information or find out which agencies contributed it. State law also establishes a process by which an individual may challenge the accuracy or completeness of the data.[12] However, we found:

- **The classification of some CIBRS data could make it difficult for individuals to take advantage of the process for learning what data CIBRS contains about them.**

Individuals can learn whether they are the subject of data in CIBRS and obtain private data about themselves by making a request to BCA or any participating agency.[13] But CIBRS data are not public, including information about participating agencies. As a result, individuals cannot easily learn the agencies other than BCA from which they can request access to CIBRS data about them. While BCA's Web site includes instructions for requests by data subjects, persons who are unable to make an in-person request to BCA must send a

[11] *Minnesota Statutes* 2012, 299C.40, subd. 6(a). Data subjects can also request the disclosure of CIBRS data about them to a third party, as provided by *Minnesota Statutes* 2012, 299C.40, subd. 6(b). As of July 2012, it appeared that few data subjects had made requests to any participating agency for CIBRS data about them or for the release of CIBRS data to a third party.

[12] *Ibid.*, subd. 7.

[13] *Ibid.*, subd. 6(a).

notarized request by postal mail. The process for requesting data by mail could take several days, while in-person requests at a participating agency closer to their residence could provide a response in minutes.

RECOMMENDATIONS

The Legislature should amend* Minnesota Statutes *2012, 299C. 40, subd. 4, to classify as public the names of participating CIBRS agencies and certain aggregate data about incidents they submit.

The Bureau of Criminal Apprehension should publish information about participating CIBRS agencies on its Web site.

The names of law enforcement agencies that participate in CIBRS are not readily available to the public.

Individuals need to know the agencies they can contact to learn if they are the subject of data in CIBRS. The Legislature can make this possible by explicitly classifying as public data about agencies that participate in CIBRS. The Legislature should also classify as public aggregate data about incidents that agencies submit. These changes to the classification of CIBRS data would allow BCA to post a list of participating agencies on its Web site, along with some information about the data each agency submits, for individuals who want to make a request for private data about themselves from an agency other than BCA. It would also provide law enforcement agencies and the public a greater understanding of the general information CIBRS contains. For example, if an agency submits person information only about suspects and arrestees, that practice would be public.

Permissible Uses

The purposes for which CIBRS may be used are limited to specific work-related tasks shown in Exhibit 3.8. For example, officers may look up someone's name in CIBRS to investigate a crime and prepare a case against that person, but they may not use CIBRS to monitor that person's ongoing interactions with law enforcement in the absence of a specific investigation. Also, they may use CIBRS to conduct background investigations for sworn law enforcement positions or positions that could lead to employment as a sworn law enforcement officer, but other background checks are not authorized. State law further specifies that only BCA-certified personnel may access CIBRS data.[14] BCA requires participating agencies to adopt policies relating to appropriate use, appropriate access, and other subjects; these policies must ensure that agency personnel comply with applicable laws and BCA requirements.

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

Exhibit 3.8: Authorized CIBRS Uses

Authorized CIBRS uses are limited to six purposes listed in statutes.

- Prepare a case against a person, whether known or unknown, for the commission of a crime or other offense for which the agency has investigative authority
- Serve process in a criminal case
- Inform law enforcement officers of possible safety issues before service of process
- Enforce no contact orders
- Locate missing persons
- Conduct background investigations for persons applying for a position as a licensed peace officer or employment that could lead to a position as a licensed peace officer

SOURCE: Office of the Legislative Auditor, summary of *Minnesota Statutes* 2012, 299C.40, subd. 2; and 626.87, subd. 1.

Searching

CIBRS users begin a search by selecting one of the six permissible uses of CIBRS and entering text to reflect the reason for their search. For example, an officer investigating an offense committed by someone with the name "Ed" would select "Law Enforcement Investigation" as the permissible use and might enter "Theft, case # 12-0034" as the reason for the search. The officer would then proceed to the search screen and enter search criteria such as "ed" in the "First Name" field, as Exhibit 3.9 shows, to find incident records with such a person. The officer could make multiple attempts to find information as part of the same search—for example, entering "edward" instead of "ed" or limiting the search to incidents from certain agencies or with certain offenses. With each successive attempt to find information, CIBRS displays the number of incident records matching the search criteria but does not display any information about the incidents. (This number is shown in the "Search History" box on the left side of Exhibit 3.9.)

In fiscal year 2012, 62 users from 29 agencies searched CIBRS.

When users are satisfied with the number of returned incident records, they can choose to view them. CIBRS first displays a list of records akin to Internet search engine results; as Exhibit 3.10 shows, this screen gives certain summary information about each incident. Users can click on any of the incidents from this list and see all the information that CIBRS contains about that incident.

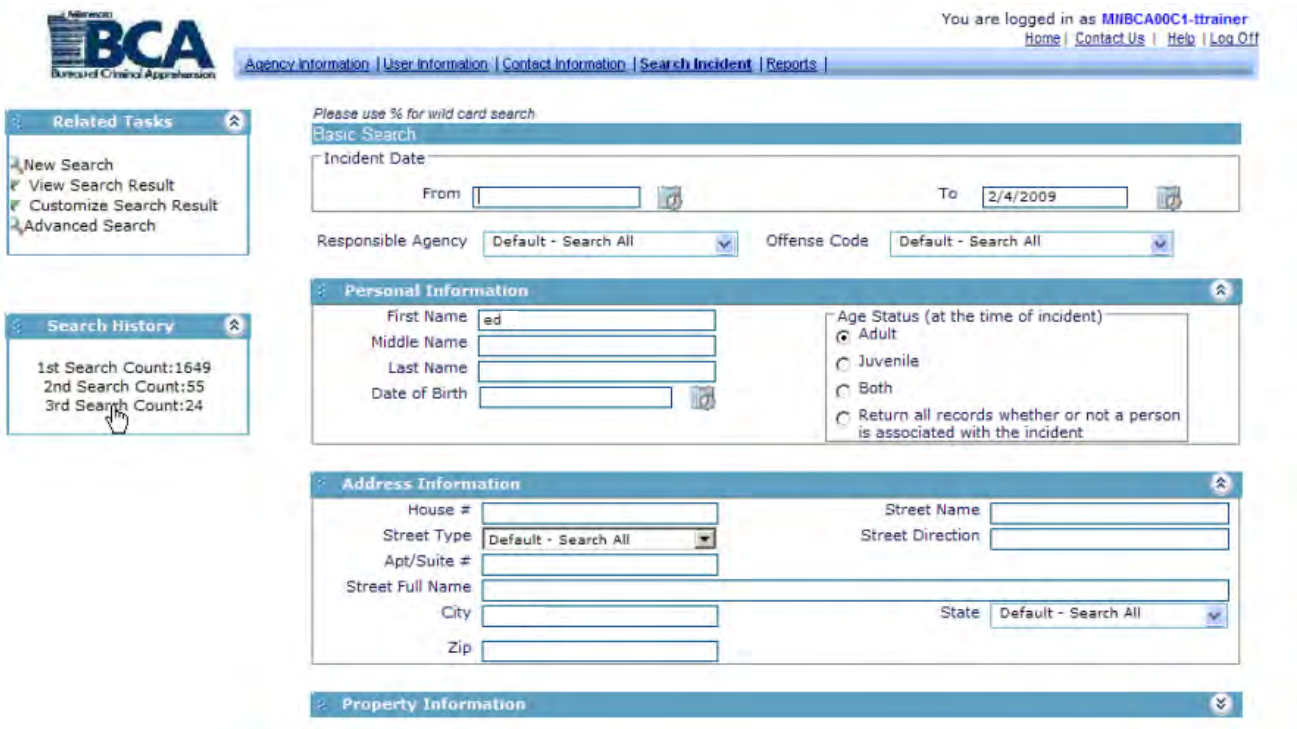
We found that:

- **Law enforcement personnel have made minimal use of CIBRS to search for information.**

As Exhibit 3.11 shows, CIBRS has not seen much use. In fiscal year 2012, for example, 62 CIBRS users collectively performed 333 searches (excluding searches testing the CIBRS system).[15] This is an average of less than one search per day. Only 29 agencies had users who searched CIBRS during the fiscal year.

[15] We defined a CIBRS "search" as all attempts within an hour of each other that a single user performed to find information for a single reason. For example, using this definition, a single search could include multiple attempts to find information about a single individual, or attempts to find information about multiple individuals for a single reason.

Exhibit 3.9: CIBRS Search Screen



NOTES: This is the basic search screen. CIBRS also has an advanced search screen, which provides more search fields. While all CIBRS data are not public, this screen shot comes from the CIBRS training, which does not contain actual CIBRS data.

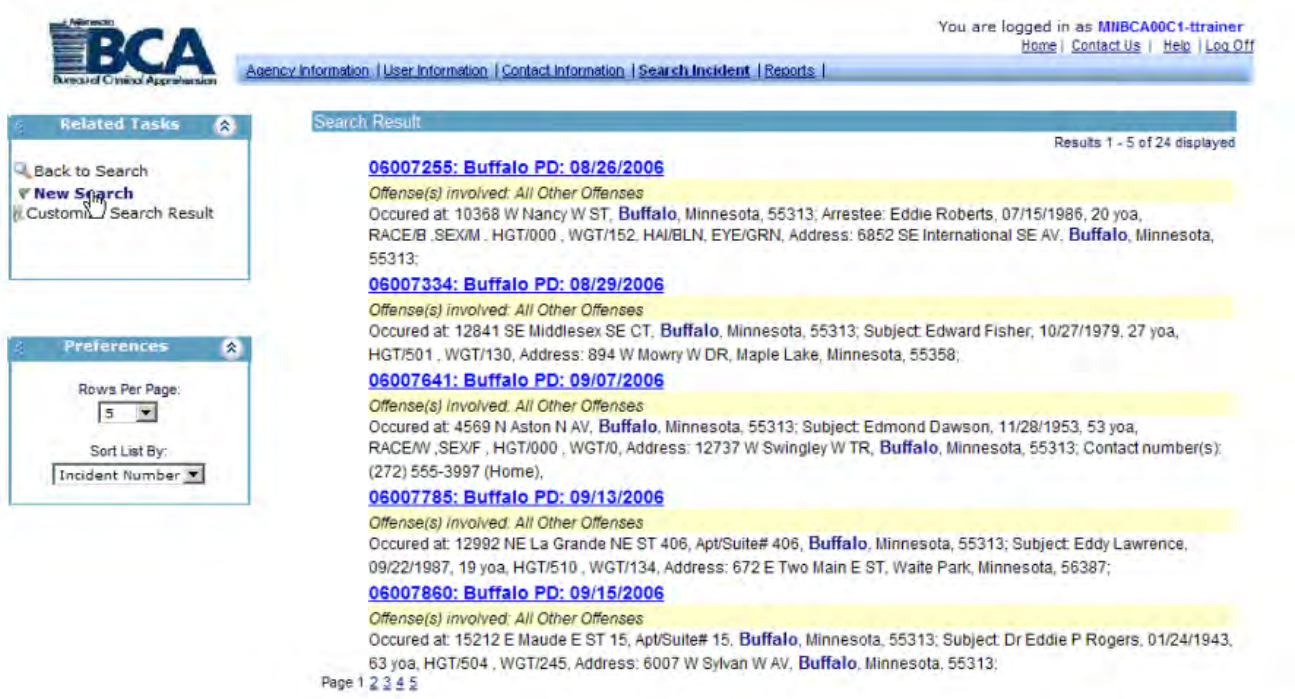
SOURCE: Bureau of Criminal Apprehension.

CIBRS use may increase because of two recent developments. First, the number of incidents in CIBRS has risen dramatically: in early 2011, CIBRS contained approximately 456,000 records; by the middle of 2012, there were 2.86 million records. Law enforcement officials at one agency we visited said that they have not used CIBRS much because they did not think it contained much data. The growing number of records may make CIBRS a more attractive search option.

Second, BCA added CIBRS to its Integrated Search Service in mid-2012.[16] Some law enforcement officials we visited told us that their staff might not search CIBRS because they have other databases available. Another said that lack of familiarity with CIBRS is an obstacle. Having the Integrated Search Service available as a more convenient way to access the data may lower these barriers.

[16] As we described in Chapter 1, the Integrated Search Service allows law enforcement personnel to search several state databases simultaneously. Individuals still need to be trained and certified to access CIBRS in order to search it using the Integrated Search Service.

Exhibit 3.10: CIBRS Search Results



NOTES: This is the summary view of results. Clicking a link will show the full detail of the associated incident. While all CIBRS data are not public, these results come from the CIBRS training database, which does not contain actual CIBRS data.

SOURCE: Bureau of Criminal Apprehension.

Exhibit 3.11: CIBRS Searches

	Fiscal Year 2012	December 2006 through June 2012
Agencies whose users performed searches	29	72
Users who performed searches	62	149
Searches[a]	333	917

NOTE: Searches performed for test purposes are not included.

[a] One CIBRS "search" represents all attempts within an hour of each other that a single user performed to find information for a single reason. For example, a single search could include multiple attempts to find information about a single individual, or attempts to find information about multiple individuals for a single reason.

SOURCE: Office of the Legislative Auditor, analysis of CIBRS data.

INAPPROPRIATE USE

As noted previously, state laws allow only BCA-certified employees of certain Minnesota law enforcement agencies to access CIBRS data, and they may do so only for limited purposes. We found:

- **Law enforcement personnel have used CIBRS in ways that statutes do not permit.**

To find instances of inappropriate CIBRS use, we examined records from CIBRS audits as well as the CIBRS audit trail.[17] We categorized searches from the audit trail as inappropriate when the user's stated reason for conducting the search clearly did not comply with state law, such as "gun permit check."[18] However, we do not know the actual circumstances of each search in the audit trail, and it is possible that some of the instances of apparent misuse we found were in fact appropriate.[19]

Misuse of CIBRS has involved work-related searches for impermissible purposes or by uncertified users.

Exhibit 3.12 shows that users from several agencies have attempted to look up over 140 names for unauthorized purposes since late 2006. For example, law enforcement personnel from seven agencies have used CIBRS to conduct background checks for more than 40 gun permit applicants. Many of these took place in 2009, but one gun permit background check occurred in June 2012.

Law enforcement personnel from three agencies have searched CIBRS to conduct inappropriate employment background checks on 48 names. Background checks are permissible in CIBRS only when they are related to sworn law enforcement positions or other positions that lead to sworn law enforcement employment.

Some users have searched CIBRS on behalf of law enforcement agencies in other states or the federal government. These agencies are not eligible to have access to CIBRS. Also, four users have searched CIBRS without BCA certification, which we defined as inappropriate use. We provide more detail on this in a later section.

---

[17] The CIBRS audit trail contains information about every search performed in CIBRS, including the identifier for the user who performed the search, the "purpose code" and reason for the search entered by the user, the search date and time, the search criterion or criteria, and identifiers for any incidents that were viewed. It also contains a record of all submissions of and changes to CIBRS data.

[18] Based on the audit files we reviewed, we believe our criterion for identifying possible misuse in the audit trail likely excludes some instances of inappropriate use. In addition, some search reasons were ambiguous. For example, the reason for one search was "chronic offender history." This search, and others with unclear search reasons, may or may not have complied with state law depending on the specific circumstances that gave rise to the search. We did not count such searches as inappropriate.

[19] This could occur if, for example, a user performed a "gun permit check" (which is not permitted) followed by a background check for a sworn officer position (which is permitted) without creating a new search. In this example, we would count two names as having been searched inappropriately when only one had been.

Exhibit 3.12: Inappropriate CIBRS Searches, December 2006 – July 2012

Type of Inappropriate Search	Agencies	Users	Searches[a]	Names Searched[b]
Background checks for gun permit applicants	7	9	38	47
Employment background checks for non-sworn positions	3	3	7	48
Searching on behalf of law enforcement agencies outside Minnesota	3	3	12	13
Searching on behalf of Minnesota law enforcement agencies without CIBRS access	2	3	17	33
Any inappropriate use	12	16	74	141

NOTES: During this time period, 149 users in 72 agencies conducted CIBRS searches that were not for testing purposes. Agencies, users, searches, and names searched can be associated with more than one type of inappropriate search. We relied on users' stated reasons for searches to classify some searches as inappropriate. We do not know the exact circumstances surrounding each of these searches, and it is possible that some were conducted for appropriate reasons.

[a] One CIBRS "search" represents all attempts within an hour of each other that a single user performed to find information for a single reason. For example, a single search could include multiple attempts to find information about a single individual, or attempts to find information about multiple individuals for a single reason.

[b] We counted what appeared to be different attempts to find information on a single person as one name. For example, we counted spelling variants (e.g., "Anderson" and "Andersen") and partial and full names (e.g., "Ed" and "Edward") as the same name.

SOURCE: Office of the Legislative Auditor, analysis of CIBRS data and audit files.

All searches described above appear to have been performed for work-related purposes, and the CIBRS audit trail contained no obvious evidence that law enforcement personnel have used CIBRS for personal reasons. Nevertheless, work-related misuse is still misuse.

TRAINING, ACCESS, AND AUDITS

Law enforcement personnel are supposed to be trained and certified before searching CIBRS.

In this section, we discuss BCA's performance in three main areas of preventing inappropriate access to and use of CIBRS: training users, limiting access to authorized users, and conducting audits to ensure agencies comply with state law and BCA policies.

Training and Certifying Users

Training helps inform users of their responsibilities as stewards of sensitive data. We found:

- **BCA has developed good policies for training CIBRS users on the appropriate uses of CIBRS data, but training content does not sufficiently address proper use of the system.**

As Exhibit 3.13 shows, BCA's approach to training CIBRS users meets most generally accepted practices. The training policy requires CIBRS users to complete BCA-provided training and pass a certification exam prior to accessing the data. They must also take the exam every two years thereafter. BCA delegates to agencies the responsibility for training and certifying users.

Exhibit 3.13: CIBRS Training Policies Compared to Generally Accepted Practices, July 2012

Most of BCA's training policies related to CIBRS are consistent with generally accepted practices.

Accepted Practice	BCA policies consistent?[a]
Train all users in policies regarding general security	Yes
Train all users in appropriate use of data	Yes
Provide refresher training	No[b]
Keep training content up to date	Yes
Maintain training and test records	Yes

NOTE: Office of the Legislative Auditor staff developed a list of best, recommended, or generally accepted practices related to sensitive data. Referenced materials included publications by: the National Institute of Standards and Technology (special publications 800-14, 800-53, 800-61, 800-92, and 800-122); the Office of Management and Budget (Memorandum 06-16, Memorandum 07-16, and Circular A-130); the U.S. Department of Justice (*Privacy, Civil Rights, and Civil Liberties Policy Development Guide: For State, Local, and Tribal Justice Entities* and *The National Criminal Intelligence Sharing Plan*); the Federal Bureau of Investigation (*Criminal Justice Information Services (CJIS) Security Policy, Version 5.0* and *National Crime Information Center (NCIC) 2000 Operating Manual*). Staff also reviewed sections of *U.S. Code* and the *Code of Federal Regulations*, as well as the Minnesota Board of Peace Officer Standards and Training Administrative Manual.

[a] Law enforcement agencies are responsible for making sure their users are trained. BCA provides training and maintains a database of certification exam results.

[b] Although BCA does not require users to take refresher training, it does require them to take a certification exam every two years.

SOURCE: Office of the Legislative Auditor.

CIBRS training is a narrated presentation that contains three short quizzes. The training covers many important topics, including data security mechanisms (such as user agreements and strong passwords), allowed purposes for searching CIBRS, and possible consequences for misuse. Training also covers data practices issues like the classification of CIBRS data, handling of requests for access to the data, and data challenges. The training alerts users that an audit trail documents all actions and that they are responsible for any searches performed using their username and password.

Though the training content is comprehensive, the apparent misuse we identified suggests that it does not effectively communicate the meaning of appropriate use. The training provides less than two minutes of narration on this material, much of which is a verbatim recitation of authorized uses outlined in state law.[20] The training does not elaborate on what the law means in practice, and it does not include concrete examples of searches that do and do not fall within the statutory definition of authorized use.

RECOMMENDATION

The Bureau of Criminal Apprehension should inform agencies and users more proactively about what constitutes appropriate CIBRS use.

[20] *Minnesota Statutes* 2012, 299C.40, subd. 2.

Gun permit background checks, unauthorized employment background checks, and searches on behalf of law enforcement agencies outside Minnesota were recurring types of misuse we identified. BCA should provide agencies and users with more guidance about appropriate CIBRS use. It could add more material on appropriate CIBRS use to its CIBRS training, such as examples of inappropriate searches and a description of how state law defines "investigations" and "access to CIBRS data." Another option is sending CIBRS agencies an annual bulletin of the kinds of misuse found in CIBRS audits and encouraging them to prevent misuse. Finally, BCA could add notes to the CIBRS initial search screen reminding users of what is permitted under each purpose code.

Participating agencies in turn need to communicate this information clearly to their CIBRS users. For example, if an agency finds that one of its users has conducted a gun permit background check, it should inform all its users, including users who gain access in the future, that this is not among the authorized uses of CIBRS.

Limiting Access

BCA delegates some responsibility for controlling CIBRS access to law enforcement agencies.

Proper administrative and technical limits are also necessary to ensure that only approved users can access CIBRS data. We found:

- **BCA has established good policies to control access to CIBRS, but participating agencies have granted access to uncertified users.**

As Exhibit 3.14 shows, BCA has created appropriate policies for limiting CIBRS access to authorized users. For example, each CIBRS user is associated with a unique identifier. This provides maximum flexibility in enabling and disabling specific privileges in CIBRS, depending on user certification.[21] It also helps provide accountability by tying all user actions to specific individuals. And, according to BCA, users can access CIBRS only from a terminal with access to the state's secure criminal justice data network. As a result, users cannot access CIBRS from their home computer.

But BCA implements its access policies by delegating a critical responsibility—ensuring that all CIBRS users are properly certified—to participating CIBRS agencies. Participating agencies must (1) sign an agreement that commits to the required training and (2) designate an agency administrator to see that users are trained and certified prior to granting or extending access. Some agencies have not fulfilled that responsibility. Between December 2006 and July 2012, 137 individuals representing 79 agencies had access to CIBRS when they lacked current certification. This number includes 38 individuals who never obtained certification (as opposed to those whose certification had expired). Four of these never-certified individuals performed a total of 17 CIBRS searches.

[21] Some users have more than one identifier because they have access privileges with more than one agency. For example, a sheriff's office employee may provide some services to smaller municipal police departments in the county. If BCA needed to disable such a user's access, it would need to disable all that user's identifiers. This could be complicated to carry out because BCA does not maintain a master list of all user identifiers held by each individual user.

Exhibit 3.14: Access Controls for CIBRS Users Compared to Generally Accepted Practices and State Law, July 2012

Accepted Practice	BCA policy consistent?
Require users to sign a user agreement	No[a]
Assign each user a unique identifier	Yes
Specify users' access rights and privileges	Yes
Disable user identifiers when user leaves organization or after periods of inactivity	Yes[b]
Limit access to certified users[c]	Yes[d]
Require strong passwords	Yes
Limit or disable remote/wireless access	Yes
Lock user account after a certain number of failed login attempts	Yes
Display notice on log-in screen warning that all actions may be monitored and summarizing the penalties for unauthorized use	Yes

NOTE: Office of the Legislative Auditor staff developed a list of best, recommended, or generally accepted practices related to sensitive data. Referenced materials included publications by: the National Institute of Standards and Technology (special publications 800-14, 800-53, 800-61, 800-92, and 800-122); the Office of Management and Budget (Memorandum 06-16, Memorandum 07-16, and Circular A-130); the U.S. Department of Justice (*Privacy, Civil Rights, and Civil Liberties Policy Development Guide: For State, Local, and Tribal Justice Entities* and *The National Criminal Intelligence Sharing Plan*); the Federal Bureau of Investigation (*Criminal Justice Information Services (CJIS) Security Policy, Version 5.0* and *National Crime Information Center (NCIC) 2000 Operating Manual*). Staff also reviewed sections of *U.S. Code* and the *Code of Federal Regulations*, as well as the Minnesota Board of Peace Officer Standards and Training Administrative Manual.

[a] BCA requires agencies to sign an agreement taking responsibility for their users' actions.

[b] BCA delegates this responsibility to law enforcement agencies.

[c] Required by *Minnesota Statutes* 2012, 299C.40, subd. 5.

[d] CIBRS locks out users who are not certified, but BCA relies on law enforcement agencies to enter users' certification status into CIBRS.

SOURCE: Office of the Legislative Auditor.

In some cases, law enforcement agencies, which are responsible for making sure their CIBRS users are trained and certified, have not done so.

BCA relies on agency administrators to record the expiration dates of users' certification in the CIBRS user database. These dates may not accurately reflect a user's true certification expiration date, which is two years after the user last passed the certification exam. While CIBRS automatically locks out users whose certification expiration dates have passed, this is incomplete protection if agency administrators enter incorrect certification expiration dates. Furthermore, the database did not require agency administrators to enter a certification expiration date to activate a user until late 2011.

Some of these instances of improper access appear to be unintentional. If an agency administrator adds many users as a batch, he or she may overlook some uncertified users. Or administrators might enter a certification expiration date that is two years from the date on which they activate a user, rather than two years from the date on which the user actually passed the exam.

But in other cases, agency administrators apparently intended to circumvent the system by entering false certification expiration dates into CIBRS. In one agency, an administrator gave a user eight consecutive one-month extensions of CIBRS access by entering new certification expiration dates. In another agency, an administrator gave a user a two-year extension and, 19 months later, an additional one-year extension.

RECOMMENDATION

The Bureau of Criminal Apprehension should ensure that only properly certified law enforcement personnel can access CIBRS.

BCA needs to see that all users with access to CIBRS are properly certified, in accordance with state law. Its current practice of relying on agency administrators to enter users' certification expiration dates has allowed users to access CIBRS without necessarily being informed of the permissible uses. During our evaluation, we notified BCA of several users who had CIBRS access in July 2012 but did not appear to have current certification. BCA deactivated these users and directed its auditors to follow up with the responsible agencies to reinforce the policy. Without implementing additional controls, however, BCA cannot guarantee that all law enforcement personnel with CIBRS access have been properly certified. That actual use of CIBRS has been minimal should not dissuade BCA from making changes, since these problems could be magnified if use increases.

BCA should ensure that CIBRS users have been trained and have current certification.

BCA maintains a database of users' certification exam results and should consider linking it to the CIBRS database. This would ensure that CIBRS would automatically control access with the correct certification expiration date, but it could be technically difficult in practice. Another option is for BCA to perform random assessments of user certifications by comparing the certification expiration dates recorded by agency administrators to the actual certification exam dates from the exam database. It could deactivate any users without current certification. This would prevent some uncertified users from having access to CIBRS, though it would not eliminate all such problems. Participating agencies would also need to be more vigilant about providing CIBRS access only to users who are properly certified, as they have agreed to do by participating in CIBRS.

Audits

As a condition of gaining access to CIBRS, law enforcement agencies agree to BCA audits that examine their compliance with applicable laws and policies.[22] BCA maintains an audit trail of all CIBRS search activity, consistent with state law.[23] CIBRS audit protocols include examining whether an agency has the required policies and whether all users have been trained and certified. If an

[22] BCA does not audit the accuracy of CIBRS data.

[23] *Minnesota Statutes* 2012, 299C.40, subd. 4(h).

agency's users have conducted searches, BCA also asks agencies to explain why some or all of them were performed.

CIBRS audits have found some misuse.

Since CIBRS came online in late 2006, BCA has completed 141 CIBRS audits, as Exhibit 3.15 shows. Almost all have been conducted remotely, not on-site. BCA has found administrative compliance issues such as incomplete policies in four of these audits, and usage compliance issues such as inappropriate searches in ten audits.[24] Agencies sometimes remedy administrative compliance issues, such as incomplete policies, during the audit. If they do not, or if there are usage compliance issues, agencies must submit written plans detailing how they will prevent such issues in the future. BCA staff said that their goal is to coach agencies into compliance. According to BCA policy, agencies might face sanctions for misuse that is intentional or is unintentional and repeated. BCA has not issued sanctions for compliance issues found in CIBRS audits.

Exhibit 3.15: CIBRS Audits, Fiscal Years 2007-12

	Audits Completed	Audits With Administrative Compliance Issues[a]	Audits With Usage Compliance Issues[b]
2007	1	0	0
2008	4	0	0
2009	11	0	0
2010	44	2	5
2011	42	1	1
2012[c]	39	1	4
Total	141	4	10

NOTE: Compliance issues reflect BCA's findings, not OLA's judgment.

[a] Administrative compliance issues noted by BCA include incomplete policies and having a user without current certification.

[b] Usage compliance issues noted by BCA include CIBRS searches for unauthorized purposes and inability to document why searches were conducted. Audits examine usage compliance issues only if an agency has performed any CIBRS searches; there were 92 such audits during this time period.

[c] Does not include June 2012.

SOURCE: Office of the Legislative Auditor, analysis of BCA's CIBRS audit files.

We found:

- **BCA's practices for auditing CIBRS use do not adequately detect and address violations of state law.**

BCA has not implemented its CIBRS audit program effectively, which has allowed conditions that violate state law to persist. Below, we discuss problems with scheduling audits, detecting inappropriate access, and detecting inappropriate use.

[24] Agencies themselves sometimes reported compliance issues during audits.

Scheduling Audits

BCA has not coordinated its CIBRS audits to ensure timely examinations of agencies' compliance. BCA's intention has been to begin initial CIBRS audits within six months of an agency's CIBRS activation, though BCA staff sometimes postpone audits by up to six months to align them with FBI-mandated audits of other databases. As Exhibit 3.16 shows, however, 55 percent of CIBRS agencies were not audited in their first 12 months of participation.[25] An additional 8 percent have never been audited, including some agencies that have granted CIBRS access to uncertified users.[26] BCA also did not complete some 2010 audits in which materials submitted by agencies showed evidence of problems, such as a search not permitted by law. According to BCA staff, this was due to a temporary lack of staff available for CIBRS audits.

Most CIBRS audits have not been initiated in a timely manner.

Exhibit 3.16: Timeliness of Initial CIBRS Audits

Months after agency activation that agency's first audit was initiated	Agencies	Percentage
Within 6 months	20	15%
More than 6 months but within 12	30	22
More than 12 months	74	55
Never audited[a]	11	8
Total	135	100%

NOTES: BCA's intention has been to begin initial CIBRS audits within six months of an agency's CIBRS activation. If an FBI-mandated audit is scheduled within 12 months of an agency's CIBRS activation, BCA may postpone the CIBRS audit so that it can be conducted in tandem with the FBI-mandated audit. This exhibit includes only those agencies that became active in CIBRS by November 15, 2011, and should therefore have been audited by November 15, 2012. We excluded two agencies from this analysis—one because it was active for only one week and one because it handles mostly technical issues.

[a] BCA had not initiated an audit with agencies in this category as of November 15, 2012.

SOURCE: Office of the Legislative Auditor, analysis of BCA's CIBRS audit files.

In 2011, BCA divided responsibility for CIBRS audits among more staff and introduced an electronic audit tool that helps it track the progress of audits. These changes appear to have helped BCA coordinate its CIBRS audits. Of the nine agencies that began participating in CIBRS between January 1, 2011, and November 15, 2011—agencies that should have received an initial audit by the time of this writing—seven received their initial audit within 12 months of gaining access to CIBRS. Nevertheless, two were not audited, including one that received an FBI-mandated audit in 2012.

[25] We limited this analysis to agencies that began participating in CIBRS by November 15, 2011, and should therefore have been audited by November 15, 2012. We excluded two agencies from this analysis—one because it was active for only one week and one because it handles mostly technical issues.

[26] Eight of the eleven agencies in this category still had access to CIBRS in July 2012.

Detecting Inappropriate Access

BCA's approach to auditing CIBRS use can miss inappropriate access and use that might occur between audits.

BCA's audit approach has rarely detected users who have CIBRS access but lack current certification. We found that 26 individuals had CIBRS access without current certification when BCA initiated audits with their agencies. Auditors detected only one of these people, who did not have a certification expiration date recorded in the CIBRS database.[27] This suggests that auditors do not check the certification expiration dates agency administrators enter in CIBRS against the actual dates.

Another source of the problem is that infrequent audits are the only tool BCA uses to detect such users. That is, even if auditors had verified users' certification dates for the agencies they audited, many more users without current certification would have gone undetected because BCA did not audit the agencies of those users when the users had CIBRS access.

Detecting Inappropriate Use

BCA auditors' method of reviewing CIBRS searches cannot detect all forms of misuse. BCA asks agencies to justify searches by providing the reason for their search (e.g., "burglary investigation"), a case number if applicable, and the role in the incident of each queried person. But agencies do not always provide complete justifications, and BCA auditors have not always required more information. For example, an auditor did not follow up with an agency about justifications stating only the reason for the search but not the role in the incident of the queried person. Similarly, another auditor did not request more information when an agency justified searches of multiple names with only the word "investigation" and a case number.

Auditors may also be unaware of precisely what kinds of searches state law allows. For example, one auditor did not identify as noncompliant several CIBRS searches performed on behalf of law enforcement personnel outside Minnesota. BCA instructs auditors to determine the reasons for searches but does not have written guidelines for identifying reasons that may be noncompliant with the law. Without more specific guidance on what state law allows, auditors may not be able to detect violations of state law.

Furthermore, BCA does not require its auditors to verify independently the search reasons provided by agencies. Independent reviews, while potentially costly and complicated by issues such as data practices, can detect problems that relying on agency justifications cannot. In one on-site audit that BCA performed in 2009, the auditor's independent review of queries found that the agency could not substantiate its justification for a search.

[27] Another user without a certification expiration date was deactivated during a different audit, but there is no documentation that this resulted from the audit.

RECOMMENDATION

The Bureau of Criminal Apprehension should improve its CIBRS audit practices by:

- ***auditing CIBRS agencies within their first six months of participation;***
- ***strengthening its auditors' reviews of CIBRS searches; and***
- ***periodically monitoring the CIBRS audit trail to identify and correct misuse between full audits.***

BCA should improve its CIBRS audit practices.

BCA needs to ensure that agencies that have recently gained access to CIBRS are operating in accordance with state laws and BCA policies. During their first several months of participation, agencies are particularly vulnerable to violations in three respects. First, they might not have all required policies in place and consequently lack documented procedures for responding to data subject requests or disciplining personnel who misuse CIBRS. Second, if agency administrators create many new user accounts at once, they could inadvertently grant access to uncertified users. Third, as users get accustomed to a new search tool, they might unintentionally use it for unauthorized purposes. Conducting audits within agencies' first six months of participation could detect these problems and prevent them from going on for years.

BCA also needs to improve the way its auditors review searches. At a minimum, BCA should direct its auditors to obtain complete justifications for audited searches by following up with agencies that provide incomplete justifications. BCA should also provide its auditors with improved guidance on what kinds of searches comply with state law. For example, BCA could reinforce to its auditors that although searches conducted for law enforcement agencies outside Minnesota may still relate to law enforcement investigations, state law does not allow those agencies to access CIBRS data.

BCA should also supplement its regular CIBRS audits with periodic monitoring, particularly to detect misuse. Certain kinds of misuse are easy to detect by monitoring the audit trail. For example, searches containing the words "gun" and/or "permit" in users' descriptions of their searches could be unauthorized gun permit checks. Auditors could review the audit trail periodically to find these and other questionable searches and follow up with any agencies performing them to prevent future occurrences.[28]

[28] This will detect some unintentional misuse but will not detect unauthorized searches that do not contain certain key words in the reference text. Monitoring is therefore no substitute for improved review of searches during audits.

CONCLUDING REMARKS

As we outlined in Chapter 1, when the Legislature wrote the CIBRS section of statutes it included provisions to balance public safety needs to share information with concerns about civil liberties and privacy. Creating the database through the legislative process contributed to transparency. BCA has established policies for CIBRS that are consistent with state law. In this section, we consider how the state has balanced these interests. We concluded that:

- **The state has designed reasonable provisions to balance policy interests surrounding CIBRS, but their cumulative effect may be limiting CIBRS' potential.**

Generally, state law and BCA policies have attended to policy interests in many ways. For example, state law allows law enforcement agencies to share incident information via CIBRS (meeting public safety needs) but limits who can access the information and the purposes for which they can use it (protecting civil liberties). State law also classifies the information as not public and allows individuals to access and challenge private information under certain conditions (addressing privacy concerns). BCA policies are designed to implement these requirements and create other practices, such as periodic audits of CIBRS use.

In this chapter, we focused on training requirements, access controls, and auditing. Overall, we think that these mechanisms are appropriate, and that BCA has crafted good policies that reflect state law. Given the inappropriate access and use we found, though, we think improved implementation of these policies is needed to better protect privacy and civil liberties.

It is less clear that legislative provisions effectively balance policy interests. CIBRS participation is voluntary: only one-third of eligible agencies participate in CIBRS, and those that do submit different subsets of incidents and information. As for data classification, CIBRS data are not public, and very little of them are confidential. Low participation and the absence of confidential data may reflect agencies' discomfort with sharing information. But low participation might also reflect agencies' reluctance to take part in a database that they perceive as containing relatively little information. The requirements of training, certification, and management of data practices issues may represent an additional disincentive. Whatever the causes, the lack of participation and the omission of information could limit CIBRS' usefulness for public safety needs. There are also less obvious costs to transparency. Although CIBRS is described in statutes, statutes do not give the public a clear sense of what the system actually contains.

Potentially, BCA could enhance transparency without negatively affecting public safety, privacy, or civil liberties by providing information about the agencies that participate in CIBRS, the general categories of information they submit (such as types of incidents and persons), and the point in the criminal justice process when the incidents are submitted. (Earlier in this chapter, we recommended a change to state law that would make such information public.) BCA could also provide summary information about the findings of CIBRS audits.

We did not make other recommendations for changing the current balance of policy issues, in part because we did not systematically evaluate why participation is low. We heard some positive comments about the CIBRS system from the few CIBRS users with whom we spoke, including that CIBRS is easy to use, that the requirement to indicate reasons for searches helps with documentation, and that the system has yielded good information. In addition, according to BCA staff, numerous stakeholders representing a variety of interests helped develop CIBRS to meet public safety needs while addressing other concerns.

The state could perhaps increase participation in CIBRS, and thus the public safety benefits of the system, by lessening the administrative burden on agencies that only submit information. As we described, every CIBRS agency must take responsibility for training and certifying users, demonstrate compliance during occasional audits, and (possibly) respond to data subjects' requests for access to CIBRS data. These procedures are important for agencies with personnel who search CIBRS, but it is less clear that they are necessary for agencies that only contribute records.

BCA may need to collaborate with law enforcement associations to make CIBRS a system that law enforcement agencies will embrace more fully than they have to this point. Working together, these groups could identify the key reasons law enforcement agencies are not participating in CIBRS. Some remedies might be ones they can agree on themselves. For example, to promote more consistent information across agencies, they could recommend certain kinds of incidents and specific data that agencies should submit. If any barriers to participation can be addressed only with changes to the CIBRS section of statutes, BCA and law enforcement representatives should bring proposals to the Legislature for public discussion through the legislative process to ensure that all policy interests are considered. Making policy about law enforcement's use of state databases ultimately requires difficult decisions about important policy interests that cannot be made with empirical information alone.

List of Recommendations

- To increase awareness of permissible uses of driver's license data:
  - The Department of Public Safety (DPS) should find additional ways to make information about permissible uses available;
  - Chief law enforcement officers should consider requiring their employees who use driver's license data to take training on the topic; and
  - DPS should work with the Sheriffs' Association and Chiefs of Police Association to develop a model policy for driver's license data use. (p. 32)
- The Department of Public Safety should strengthen controls over law enforcement users' access to driver's license information. (p. 33)
- Chief law enforcement officers should consider doing more proactive monitoring of their employees' use of driver's license data. (p. 41)
- The Department of Public Safety should consider investing additional resources to monitor use of driver's license data and formalizing its approach to handling inquiries into use of these data. (p. 41)
- The Legislature should amend *Minnesota Statutes* 2012, 299C. 40, subd. 4, to classify as public the names of participating CIBRS agencies and certain aggregate data about incidents they submit. (p. 53)
- The Bureau of Criminal Apprehension should publish information about participating CIBRS agencies on its Web site. (p. 53)
- The Bureau of Criminal Apprehension should inform agencies and users more proactively about what constitutes appropriate CIBRS use. (p. 59)
- The Bureau of Criminal Apprehension should ensure that only properly certified law enforcement personnel can access CIBRS. (p. 62)
- The Bureau of Criminal Apprehension should improve its CIBRS audit practices by:
  - auditing CIBRS agencies within their first six months of participation;
  - strengthening its auditors' reviews of CIBRS searches; and
  - periodically monitoring the CIBRS audit trail to identify and correct misuse between full audits. (p. 66)

Law Enforcement Agencies

APPENDIX

We conducted three discussion groups with representatives from law enforcement agencies. We also completed ten on-location site visits and corresponded with one additional site-visit agency. Site visits included meetings or correspondence with the agency's chief law enforcement officer and/or other staff.[1] The agencies who participated represented agencies of various sizes, geographic locations, and jurisdiction, as shown in Exhibit A.1.

Exhibit A.1: Law Enforcement Agencies

	Group Discussion	Site Visit	Ride Along
Police Departments			
Albert Lea		X	
Alexandria		X	
Cannon Falls	X		
Crookston	X		
Duluth	X		
Forest Lake	X		
Gilbert (serving Gilbert and Biwabik)		X	X
Howard Lake	X		
Isanti	X		
Montevideo	X		
Plymouth	X		
Robbinsdale		X	X
Roseville	X		
Spring Lake Park	X		
Three Rivers Park District	X		
Windom		X	
Sheriff's Offices			
Cass County		X	
Hennepin County	X		
Kandiyohi County	X		
Olmsted County	X		
Polk County		X	
Ramsey County		X	
Swift County		X	
State Law Enforcement Agencies			
Bureau of Criminal Apprehension	X		
Department of Corrections Fugitive Apprehension Unit	X	X	
Department of Natural Resources Enforcement Unit	X		
State Patrol	X	X	X

SOURCE: Office of the Legislative Auditor.

[1] Although not a site-visit agency, the Roseville Police Department met with us early in the evaluation to talk about how law enforcement personnel use information.

Office of the Commissioner

445 Minnesota Street • Suite 1000 • Saint Paul, Minnesota 55101-5100
Phone: 651.201.7160 • Fax: 651.297.5728 • TTY: 651.282.6555
www.dps.state.mn.us

Alcohol and Gambling Enforcement

Bureau of Criminal Apprehension

Driver and Vehicle Services

Emergency Communication Networks

Homeland Security and Emergency Management

Minnesota State Patrol

Office of Communications

Office of Justice Programs

Office of Traffic Safety

State Fire Marshal

February 5, 2013

James Nobles, Legislative Auditor
Office of the Legislative Auditor
658 Cedar Street, Room 140
St. Paul, Minnesota 55155

Dear Mr. Nobles:

Thank you for your analysis and subsequent report regarding use of state databases by the law enforcement community. As you acknowledge in your analysis, sensitive information must be available to law enforcement officers in order for them to carry out their public safety responsibilities and solve crime. We strongly agree that this data should not be accessed in a manner that violates the trust the citizens of our state have a right to expect.

The report recommends increased oversight and user training; we commit to strengthening our efforts on both fronts. However, it is important to recognize 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. The Department of Public Safety will continue to stress to all users the importance of accessing this data in a legal and ethical manner.

We appreciate your recommendations and will address each with appropriate strategies. While our efforts will continue to evolve, we are currently undertaking the following:

- Training on proper use of driver license data has been and will continue to be provided to all users. All police officers with authorized access to Driver and Vehicle Services (DVS) data will be expected to complete online training, developed by our DVS division.
- DPS is working cooperatively with Chief Law Enforcement Officers throughout the state in the development of policies for proper use of the system, ensuring officers are properly trained, conducting routine audits of officer access to, and the use of the data, and procedures to ensure individuals leaving employment no longer are able to access the system.
- Restrict law enforcement officer's access to historical photos.
- The Bureau of Criminal Apprehension (BCA) will incorporate training regarding permissible uses of driver license information into existing training provided to police officers.

- The BCA is working to implement an audit tool that will proactively monitor usage patterns for driver license data accessed through the BCA. Initial testing of the audit tool has shown that this is a complex endeavor that will take time to develop.
- DVS is implementing a new driver and vehicle information system that includes "Identity Access Management" which will strengthen our oversight of appropriate use of the data.
- The BCA will modify its Comprehensive Incident Based Reporting System (CIBRS) training and supporting materials to provide more examples of appropriate and inappropriate use of CIBRS data.
- The BCA will take steps to ensure that only properly certified law enforcement personnel can access CIBRS, including review of certified and active users during the CIBRS audit.
- The BCA will improve its CIBRS audit practices by auditing agencies within their first six months of participation in order to strengthen the review done by auditors of CIBRS searches. Additionally BCA will periodically monitor the CIBRS audit trail to identify and correct misuse between full audits.
- The BCA will publish information about the agencies that participate in the submission of data to CIBRS, and the aggregate data about the incidents those agencies submit, if the legislature decides to make a statuary change; however, the BCA is concerned that publication of this type of information may discourage some agencies from submitting data which will result in less information being available to law enforcement agencies, for investigative purposes.

Thank you for your insights and the work of your staff. Please know that we continue to do all that we can to ensure the citizens of our state that their data will be properly protected.

Sincerely,

Ramona L. Dohman
Commissioner

Forthcoming Evaluations

Medical Assistance Payment Rates for Dental Services, March 2013
Special Education, March 2013
State-Operated Human Services, February 2013

Recent Evaluations

Agriculture
"Green Acres" and Agricultural Land Preservation Programs, February 2008
Pesticide Regulation, March 2006

Criminal Justice
Law Enforcement's Use of State Databases, February 2013
Public Defender System, February 2010
MINNCOR Industries, February 2009
Substance Abuse Treatment, February 2006
Community Supervision of Sex Offenders, January 2005
CriMNet, March 2004

Education, K-12, and Preschool
K-12 Online Learning, September 2011
Alternative Education Programs, February 2010
Q Comp: Quality Compensation for Teachers, February 2009
Charter Schools, June 2008
School District Student Transportation, January 2008

Education, Postsecondary
Preventive Maintenance for University of Minnesota Buildings, June 2012
MnSCU System Office, February 2010
MnSCU Occupational Programs, March 2009
Compensation at the University of Minnesota, February 2004

Energy
Renewable Energy Development Fund, October 2010
Biofuel Policies and Programs, April 2009
Energy Conservation Improvement Program, January 2005

Environment and Natural Resources
Conservation Easements, February 2013
Environmental Review and Permitting, March 2011
Natural Resource Land, March 2010
Watershed Management, January 2007

Financial Institutions, Insurance, and Regulated Industries
Liquor Regulation, March 2006
Directory of Regulated Occupations in Minnesota, February 1999
Occupational Regulation, February 1999

Government Operations
Helping Communities Recover from Natural Disasters, March 2012
Fiscal Notes, February 2012
Capitol Complex Security, May 2009
County Veterans Service Offices, January 2008
Pensions for Volunteer Firefighters, January 2007
Postemployment Benefits for Public Employees, January 2007

Health
Financial Management of Health Care Programs, February 2008
Nursing Home Inspections, February 2005
MinnesotaCare, January 2003

Human Services
Child Protection Screening, February 2012
Civil Commitment of Sex Offenders, March 2011
Medical Nonemergency Transportation, February 2011
Personal Care Assistance, January 2009
Human Services Administration, January 2007
Public Health Care Eligibility Determination for Noncitizens, April 2006

Housing and Local Government
Consolidation of Local Governments, April 2012
Preserving Housing: A Best Practices Review, April 2003
Managing Local Government Computer Systems: A Best Practices Review, April 2002
Local E-Government: A Best Practices Review, April 2002
Affordable Housing, January 2001

Jobs, Training, and Labor
Workforce Programs, February 2010
E-Verify, June 2009
Oversight of Workers' Compensation, February 2009
JOBZ Program, February 2008
Misclassification of Employees as Independent Contractors, November 2007
Prevailing Wages, February 2007

Miscellaneous
The Legacy Amendment, November 2011
Public Libraries, March 2010
Economic Impact of Immigrants, May 2006
Gambling Regulation and Oversight, January 2005
Minnesota State Lottery, February 2004

Transportation
Governance of Transit in the Twin Cities Region, January 2011
State Highways and Bridges, February 2008
Metropolitan Airports Commission, January 2003

Evaluation reports can be obtained free of charge from the Legislative Auditor's Office, Program Evaluation Division, Room 140 Centennial Building, 658 Cedar Street, Saint Paul, Minnesota 55155, 651-296-4708. Full text versions of recent reports are also available at the OLA Web site: http://www.auditor.leg.state.mn.us