Concealed Handgun Permit Database
Colorado Bureau of Investigation
Department of Public Safety

Performance Audit
November 2010

OFFICE OF THE
STATE AUDITOR

LEGISLATIVE AUDIT COMMITTEE
2010 MEMBERS

Senator David Schultheis
Chair

Senator Lois Tochtrop
Vice-Chair

Senator Morgan Carroll
Representative Jim Kerr
Representative Joe Miklosi

Senator Shawn Mitchell
Representative Dianne Primavera
Representative Mark Waller

OFFICE OF THE STATE AUDITOR

Sally Symanski
State Auditor

Cindi Stetson
Deputy State Auditor

Eric Johnson
Jonathan Trull
Legislative Audit Managers

Cassi Clark
Nina Frant
Reed Larsen
Nathan White
Legislative Auditors

The mission of the Office of the State Auditor is to improve the efficiency, effectiveness, and transparency of government for the people of Colorado by providing objective information, quality services, and solution-based recommendations.

Office of the State Auditor

Sally Symanski, CPA
State Auditor

November 18, 2010

Members of the Legislative Audit Committee:

This report contains the results of a performance audit of the Concealed Handgun Permit Database. The audit was conducted pursuant to Section 2-3-103, C.R.S., which authorizes the State Auditor to conduct audits of all departments, institutions, and agencies of state government, and Section 2-3-118, C.R.S., which requires the State Auditor to conduct a performance audit of the concealed handgun permit database. The report presents our findings, conclusions, and recommendations, and the responses of the Department of Public Safety and the Colorado Bureau of Investigation.

Sally Symanski

This page intentionally left blank.

Concealed Handgun Permit Database

Purpose and Scope

Statute [Section 2-3-118, C.R.S.] requires the State Auditor to conduct an audit by January 1, 2011, of the statewide database of concealed handgun permittees maintained by the Colorado Bureau of Investigation (CBI) in the Department of Public Safety (Department). According to statute, the performance audit is to address:

- The security of the information contained in the database,
- The accuracy of the information contained in the database, and
- The benefits of the database for Colorado law enforcement and for public safety.

To determine the security of the information in the database, we reviewed the physical and logical security of the Colorado Crime Information Center (CCIC) system, in which the database resides. Our audit work included onsite visits to CCIC's production and disaster recovery locations, interviews with staff, and attempts to gain logical access to the system. In addition, we contracted with a security firm that attempted to gain unauthorized access to the CCIC system as part of our assessment of the system's security. We also reviewed user access controls, such as the addition and termination of users.

To determine the accuracy of the information in the database, we evaluated the reliability of the information contained in the database for verifying the validity of a permit, which is the purpose of the database as set forth in statute [Section 18-12-206(3)(a), C.R.S.]. Our reliability assessment included reviewing the database for accuracy (e.g., errors, duplicate records, expired records, and inconsistent data) and completeness. We also evaluated the adequacy of controls (e.g., edit checks) designed to limit data entry errors and ensure data integrity. We did not review files, such as concealed handgun permit applications, at county sheriffs' offices, which are responsible for issuing concealed handgun permits and entering permit information into the database. The Office of the State Auditor does not have the authority to audit local governments, including local law enforcement agencies.

To address the benefit of the database for law enforcement and public safety, we surveyed and interviewed law enforcement and other stakeholders to obtain their perceptions of the benefits. We also participated in ride-alongs with law enforcement officers. Overall we were not able to obtain sufficient, appropriate evidence to conclude on whether the database provides a benefit to law enforcement or public safety.

The audit work was performed from April through November 2010 and was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background on Concealed Handgun Permits

Colorado case law defines a concealed handgun as one that is “placed out of sight so as not to be discernable or apparent by ordinary observation.” Colorado is one of 48 states that allows individuals to carry concealed handguns. These states have laws that vary widely in terms of how strictly they regulate the permitting and carrying of concealed handguns. Under current law [Section 18-12-203, C.R.S.], Colorado’s 64 sheriffs are the only members of law enforcement that have authority to issue concealed handgun permits in the state. According to statute [Section 18-12-203(1), C.R.S.], sheriffs must issue a concealed handgun permit if the applicant:

- Is a legal resident of Colorado,
- Is at least 21 years old,
- Is not ineligible to possess a firearm (which includes handguns) pursuant to state and federal law (e.g., has not been convicted of a crime punishable by more than one year of imprisonment),
- Is not subject to a protection order,
- Has not been convicted of perjury,
- Does not chronically or habitually use alcohol,
- Is not an unlawful user of or addicted to a controlled substance, and
- Demonstrates competence with a handgun (requires a proof of training certificate).

Even if a person meets the criteria listed above, statute allows the sheriff discretion to deny, revoke, or refuse to renew a permit if the sheriff has a reasonable belief that documented previous behavior by the applicant makes it likely the applicant will present a danger to self or others if the applicant receives a permit to carry a concealed handgun [Section 18-12-203, C.R.S.]. If the sheriff denies, revokes, or refuses to renew a permit, the applicant has the right to seek judicial review and the sheriff bears the burden of proof that the applicant is ineligible to possess a permit [Section 18-12-207, C.R.S.].

Permits are valid for five years and allow a person to carry a concealed handgun in all areas of the state except in places where the carrying of firearms is prohibited by federal or state law. Statute prohibits the carrying of concealed handguns on school property (elementary through high school), in a public building where all people are screened and required to leave weapons with security personnel at the entrance, and on private property where concealed handguns are not allowed by property owners [Section 18-12-214, C.R.S.]. Carrying a concealed handgun is legal without a permit if a person is hunting, in his or her own home, or in a private vehicle when carrying the weapon for legal purposes, including self-defense [Section 18-12-204(3)(a), C.R.S.]. Local governments may prohibit the *open* carrying of firearms in a building or specific area within their jurisdictions [Section 29-11.7-104, C.R.S.], but they cannot restrict the carrying of concealed handguns [Section 18-12-214(1)(a), C.R.S.].

The number of concealed handgun permits issued by sheriffs in Colorado has increased over the past five years. According to data from the County Sheriffs of Colorado (a professional association), in Calendar Year 2005 Colorado sheriffs issued about 6,300 permits compared to about 27,000 permits in Calendar Year 2009, an increase of 329 percent. In total, sheriffs issued approximately 67,000 permits from Calendar Years 2005 through 2009; however, as we explain later, not all of these permits are recorded in the concealed handgun permit database.

Concealed Handgun Permit Database

Senate Bill 03-024, which created statewide standards for issuing concealed handgun permits, authorized the creation of a temporary statewide database of concealed handgun permittees. As a result of the bill, statute [Section 18-12-206(3)(a), C.R.S.] establishes that (a) sheriffs must maintain a list of the persons to whom they issue permits; (b) sheriffs may, at their discretion, share information from their list of permittees with other law enforcement "for the purpose of determining the validity of a permit"; and (c) a database of permittees, composed of information provided by the sheriffs, may be maintained by a state agency as long as the database is searchable by name only. This section of statute does not give CBI specific authority to determine the type of information that should be included in the database, nor does it specifically name CBI as the state agency responsible for maintaining the database. Statute [Section 18-12-206(3)(b)(I), C.R.S.] also requires the database to sunset and all information about concealed handgun permittees to be removed from any statewide database by July 1, 2011.

As mentioned previously, the concealed handgun permit database resides in CCIC, which is the statewide criminal justice computer system managed by CBI.

CCIC includes information about statewide and national warrants, criminal history records, driver's licenses, missing persons, protected parties, stolen property, sex offenders, and intelligence. In addition, the system acts as an interface with other federal, state, and local criminal justice databases. Within CCIC, the concealed handgun permit database is a table, the contents of which are available for viewing by CCIC users, including Colorado law enforcement agencies such as sheriffs, police, and state troopers. The concealed handgun permit database contained about 51,000 records as of May 2010.

Although the database was not specifically authorized in statute until 2003, CCIC was used to maintain records for some permit holders prior to that date. Specifically, some Colorado police chiefs, who could issue permits prior to the enactment of Senate Bill 03-024, and sheriffs made arrangements with CBI to enter their permittees' information into the "persons of interest" table in CCIC. There are currently about 3,300 records in the database from these prior arrangements; the oldest records date back to 1995. After the enactment of Senate Bill 03-024, sheriffs continued to enter permit holder information into the "persons of interest" table in CCIC. However, sheriffs raised concerns about having law-abiding concealed handgun permittees listed in the "persons of interest" table, because this table also included information about people wanted for arrest. As a result, CBI established a separate table in CCIC for concealed handgun permittee information. In 2007 CBI moved all existing concealed handgun permit records out of the "persons of interest" table and into the new table within CCIC specifically designated for concealed handgun permittee information. This table continues to hold concealed handgun permittee information and is referred to as the concealed handgun permit database.

Law enforcement can search the concealed handgun permit database two ways: through a direct search of the database or through a general search of CCIC. For a direct search of the database, the user sees only matching results of people who have concealed handgun permits. For a general search of CCIC, the user sees results from other databases within CCIC, such as warrants, driving records, missing persons, etc., in addition to concealed handgun permit information. For example, if an officer searches for a name in CCIC to view the person's driving record or to see whether the person has any outstanding warrants or criminal history, matches from the concealed handgun permit database will also be displayed. Regardless of whether a law enforcement official performs a direct search of the concealed handgun permit database or a general search of CCIC, the information retrieved is similar to the list of links returned in an Internet browser search, showing the permittee's name, date of birth, identifying information such as height and weight, and permit status (i.e., active, revoked, or denied). To read the details of the permit record, such as the permit's expiration date or notes about the permit, the officer must click on the link. Law enforcement may search the database from their cars or call dispatch to search for them.

Summary of Findings

Our audit found the concealed handgun database housed in CCIC to be physically and logically secure. However, we found the information in the database is not reliable for law enforcement to use in determining the validity of a permit, which is the stated purpose of the database in statute [Section 18-12-206(3)(a), C.R.S.]. Specifically, of the 51,000 records in the database, 32,000 (63 percent) contained inaccurate or inconsistent information. Also, the database does not contain records for about 45 percent of permits issued in the state. Finally, because quantifiable data were not available for our audit to conclude on the benefits of the database for law enforcement or public safety, we obtained information on the perceptions of law enforcement and stakeholders about the database's benefits through surveys and interviews.

The remainder of the report is divided into four sections. The next two sections address the security and accuracy of the information in the database and provide recommendations for improving the database. The third section outlines the reported benefits of the database for law enforcement and public safety, while the last section outlines database issues that policymakers may want to consider.

Database Security

Statute [Section 2-3-118, C.R.S.] requires that this audit review the security of the concealed handgun permit database. Information security is the process of designing, implementing, and maintaining controls to protect information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The Department and the Governor's Office of Information Technology (OIT) are responsible for protecting and maintaining the CCIC database. While OIT provides technical support and day-to-day maintenance of the CCIC application, the Department is ultimately responsible for the data. As previously mentioned, the concealed handgun permit database exists within the CCIC system. Therefore, we evaluated security controls over relevant components of the CCIC system, which was upgraded to a new version in May 2010. Because the CCIC system interacts with the Federal Bureau of Investigation's (FBI's) National Crime Information Center system, the CCIC system must comply with both State Cyber Security Policies and FBI standards surrounding information security. The primary objectives for our review were to determine whether:

- The Department's controls were reasonably designed and operating effectively to protect the confidentiality and integrity of permit holder information,

- Malicious individuals could circumvent the Department's controls to gain unauthorized access to permittee information, and

- The Department was complying with required FBI and State Cyber Security Policies.

Overall we concluded that the security of the concealed handgun permit database was reasonably sufficient to protect the database and permittee information from unauthorized access, use, disclosure, modification, or destruction. To reach this conclusion, we tested all relevant components of the database and the new CCIC system, including network and web application security, logical and physical access, and operating- and database-level controls. We also interviewed key staff and performed automated scans of the CCIC system and the database. Based on our work, we found that the Department's information technology controls related to the concealed handgun permit database and CCIC system are reasonably designed and operating effectively to protect the confidentiality and integrity of permit holder information.

In addition to those tests performed by our staff, we contracted with a professional computer security company to perform a penetration test of the CCIC system, including the concealed handgun permit database. A penetration test is a security assessment in which testers, acting as malicious individuals, attempt to circumvent an organization's security controls to gain unauthorized access to systems and data. The testers were unable to gain unauthorized access to either the CCIC system or the concealed handgun permit database. As such, we concluded that the permittee information was reasonably protected from unauthorized disclosure resulting from attacks by malicious individuals.

Although the Department's controls are sufficient to protect the security of the database and permittee information, we identified six areas in which the Department was not in full compliance with FBI and State Cyber Security Policies. These areas included:

- **Data encryption.** The Department has designated the data contained in the concealed handgun permit database as Level 3 data. According to State Cyber Security Policies, Level 3 is the highest, or most restrictive, data classification and requires the most stringent security controls. For Level 3 data**,** these policies require that the data be encrypted when stored on external media, such as backup tapes, and recommends that the data be encrypted while at rest in a database. Although the Department encrypts permit holder information in transit between the database and end users, it does not encrypt the data while at rest in the database or when stored on external media. This practice presents a low-level risk that the data could be readable to unauthorized individuals if other security controls fail.

- **Management of administrative accounts.** State Cyber Security Policies require that system administrators have individual accounts to perform system administrative tasks and that accounts belonging to terminated users be immediately disabled from all system components. During our testing, we found that two Department staff are sharing generic administrative accounts to perform occasional work on the CCIC system. This practice violates State Cyber Security Policies and would make it difficult to identify and hold an individual responsible should inappropriate activities, such as making unauthorized changes to data, occur with one of these accounts. Additionally, we identified an active administrative account on the CCIC test environment that belonged to a former employee. The Department immediately deactivated the account when notified by our staff.

- **Documentation of terminated users.** State Cyber Security Policies require agencies to maintain, for one year, documentation related to the termination of user access to state systems. We sampled 30 recently terminated CCIC users to ensure that the Department followed procedures and removed those users' CCIC accounts timely. Of the 30 users sampled, the Department was unable to provide sufficient documentation for 10 users (33 percent), including the reason for account removal and the date the request for account removal occurred. For the 20 terminated users with sufficient documentation, we found that the Department followed all required procedures and that the CCIC accounts for these users were removed in a timely manner.

- **Information security awareness training and information technology (IT) security reviews.** As noted previously, because the CCIC system handles and interacts with federal criminal justice and intelligence information and systems, the Department must comply with FBI information security standards. During our audit, we found that the Department has faced challenges meeting the requirements of two FBI security standards. First, the FBI requires that all CCIC users receive security awareness training at least once every three years. Although the Department provides all new users with security awareness training, the Department has not provided this training to existing users on an ongoing basis. Second, the FBI requires the Department, as CCIC's custodian, to perform an IT security review of each user agency once every three years. CCIC user agencies include local, state, and some federal law enforcement agencies. The IT security reviews are designed to ensure that user agencies are complying with FBI standards and Department user- and agency-level agreements. Due to staffing constraints, the Department has been unable to fully comply with this requirement. Currently the Department has one staff person to conduct IT security reviews at the 670 user agencies. In addition to performing IT security reviews, this staff person is also responsible for the information security operations of the Department. The FBI reviews compliance with its security standards every three years; 21 months into the FBI's current three-year compliance cycle, the Department has conducted IT security reviews at only 48 of the approximately 670 user agencies. Our July 2003 *Colorado Bureau of Investigation Performance Audit* had a similar finding and recommended that CBI take steps to comply with the FBI's IT security review requirement, which CBI agreed to do by December 2003. We also identified this same finding in a 1996 performance audit of CBI. The Department is currently working on automated solutions to address these two areas of noncompliance.

- **Server hardening.** State Cyber Security Policies require that systems be "hardened," or configured to protect sensitive information. Hardening includes removing or changing all guest accounts and default passwords, disabling nonessential services, and setting system parameters to mitigate potential attacks. To ensure that a server is properly hardened, it is important to use an established hardening guide and follow a systematic approach to ensure that areas are not missed. We found that prior to implementation of the new CCIC system in May 2010, the Department did not properly harden the relevant servers and operating systems. Department staff reported that some hardening of the new CCIC system was completed, but the hardening was done without following an established guide and approached in an ad hoc manner. In September 2010 we performed an automated assessment of the CCIC system against an approved hardening standard established by the Center for Internet Security and found that, although the system was now reasonably hardened, several areas still needed to be addressed. We provided specific details of our assessment to the Department under separate cover.

- **User access.** State Cyber Security Policies require that state agencies provide users with the least amount of access necessary to perform their job duties. Statute only allows sheriffs to issue permits and share information about those permits with other law enforcement agencies. Therefore, only sheriffs' offices have specific authority to enter information into the permit database within CCIC. We found that 26 records in the database were created by agencies that are not authorized to issue concealed handgun permits. Specifically, four different police departments created records in the database during Calendar Years 2005 through 2009. Based on our review of access controls for the permit database, we found that many non-sheriff agencies have the ability to add records to the permit database. All records entered by any law enforcement agency other than sheriffs' offices should be considered invalid, because the agency is not authorized to issue concealed handgun permits.

The Department has taken reasonable steps to ensure the security of the concealed handgun permit database, including permittee information. To further improve the security of the database, the Department should work with OIT to implement changes that will fully address those requirements, as noted in the recommendation below.

Recommendation No. 1:

The Department of Public Safety should work with the Governor's Office of Information Technology to further improve the security of the Colorado Crime Information Center (CCIC) and the concealed handgun permit database within CCIC by:

a. Encrypting data at rest in the concealed handgun permit database and when transferred to external media, if the General Assembly authorizes the continuation of the database beyond July 1, 2011.

b. Promptly removing terminated users' access from all CCIC components and environments.

c. Ensuring that administrative functions are performed with individual, non-shared accounts or through system utilities.

d. Maintaining documentation related to the termination of CCIC users.

e. Implementing the prior audit recommendation and complying with FBI security standards by performing IT security reviews of all local law enforcement user agencies every three years and providing security awareness training to all CCIC users according to FBI timelines.

f. Systematically hardening the CCIC system according to an approved standard and documenting the results.

g. Reviewing user access rights to the concealed handgun permit database and taking steps to ensure that county sheriffs' offices are the only agencies entering information into the database. In addition, the Department should review records created by police departments and remove as appropriate.

Department of Public Safety Response:

a. Agree. Implementation date: Assessment to be completed by July 2011.

   The State Cyber Security Policies set forth standards for data residing on state computer systems when data are considered at rest. The Department-assigned technology staff from the Office of Information Technology (OIT) will conduct an assessment study on methods to best encrypt the CCIC databases which will include the concealed handgun permit database. The Colorado Bureau of Investigation (CBI) will collaborate with OIT to determine if the best course of action is to implement full disk encryption, database encryption, or request a waiver from the Colorado Office of Cyber Security. The Department may need to seek additional funding in order to meet this requirement. The Department plans to encrypt data on external media.

   It should be noted that Federal Bureau of Investigation security policy, Section 5.10.1.2, requires no encryption of rest data when the data are maintained in a secured location. CCIC data are located at the CBI facility, which is a secured facility.

b. Agree. Implementation date: Implemented.

   One local administration account was identified by the audit staff which belonged to an employee that retired from the Department on May 31, 2010, that was found to be still active. This account has since been removed and the Department is now in compliance with State Cyber Security Policies.

c. Agree. Implementation date: Implemented.

   Two system administrators were identified during the audit as using a shared account to perform administrative functions in CCIC systems. Individual accounts have been created for these users to uniquely identify individual use for administrative functions. CBI is now in compliance with State Cyber Security Policies.

d. Agree. Implementation date: Implemented.

   Beginning November 3, 2010, every Operator Security Number (OSN) cancellation received over CCIC is logged in the CCIC administrative index using the date of receipt and the Master Record Index (MRI) number from the cancellation request. Using the MRI and date, CBI can identify the cancellation message in an archive file along with the exact date and time it was received by CBI. The user access was terminated for the users identified in the audit sample; however, CBI could not produce documentation as to the date and time the termination requested was received at CBI.

e. Agree. Implementation date: December 2011.

CBI implemented a vendor-hosted online security awareness training platform in July 2010 to deliver and track security awareness training. In September and October 2010 CBI provided information about the security awareness training system to all local agencies. In November 2010 CBI conducted a statewide webinar to instruct local law enforcement agencies on how to administer the training. A second webinar is planned for December 2010. CBI has added security awareness training to the mandatory recertification test for users with Operator Security Numbers (OSNs) as a prerequisite for renewing their access to CCIC.

CBI is working to implement a vendor-hosted online IT security review process for local law enforcement user agencies to augment onsite security audits. Local law enforcement user agencies will be required to complete the online self-assessment that will then be reviewed by CBI staff. Based on the results of the self-assessments, CBI staff may conduct further onsite testing. The online IT security reviews will allow CBI to meet the FBI's three-year audit requirement. The online IT security review process is now operational.

CBI anticipates meeting the training requirement prior to CBI's next FBI audit which will take place in Calendar Year 2011. CBI provided an update to the FBI Criminal Justice Information Services (CJIS) Advisory Policy Board on the progress of security awareness training on October 27, 2010.

f. Agree. Implementation date: Ongoing.

A vulnerability assessment was performed by the Colorado Office of Cyber Security (OCS) on the CCIC system prior to the upgraded CCIC system implementation in May 2010. Security hardening was performed on the CCIC servers based on the findings of an OCS vulnerability assessment. CBI will collaborate with OIT to continue the process of identifying hardening standards and will document the process within the agency cyber security plan.

g. Agree. Implementation date: Deletion of identified records by July 2011.

The CCIC message switch and associated systems are provided and maintained by the vendor, Computer Projects of Illinois (CPI). To change the message keys used to enter and maintain concealed handguns entries so that a user would be identified and validated as an employee of a sheriff's office would fall outside normal maintenance and would be an additional expense to the agency.

Although it would be possible to "set aside" the message keys on a separate part of our limited user security grid and restrict it to sheriff's office users, this would be a significant undertaking. CPI would need to identify and change the affected users which would also fall outside normal maintenance and would be an additional expense to the agency. If a technological solution is not possible, CBI would implement a manual process of reviewing user access rights and validating database entries on an annual basis. This work process change would place additional staff demands on CBI.

Looking to the future, CPI is testing changes to the user configuration tool to allow state administrators to define user access by user role. With an updated configuration tool which may be available within the next five years, it will be easier to fine-tune access for a diverse user base.

Meanwhile, the CBI Program Support Unit, working with and through the CCIC Board of Working Advisors, will address this matter as a training issue to ensure appropriate entry of records into the concealed handgun permit database. CBI will meet with police agency heads to discuss the deletion of identified records.

Database Reliability

Statute [Section 2-3-118(1), C.R.S.] requires that our audit address the accuracy of the information in the concealed handgun permit database. As noted previously, statute [Section 18-12-206(3)(a), C.R.S.] does not require sheriffs to enter information into the database, but stipulates that sheriffs may share permit information with law enforcement "for the purpose of determining the validity of a permit." Therefore, to assess the accuracy of the information in the database, we considered how reliable the information is for law enforcement to use in determining the validity of a permit. According to guidance from the United States Government Accountability Office (GAO), data reliability pertains to the accuracy and completeness of the data, given the uses for which the data are intended. The GAO further defines accuracy as the extent to which recorded data reflects the actual underlying information, and completeness as the extent to which relevant records are present and the fields in each record are populated appropriately. Consistency, as a subcategory of data accuracy, refers to data that are clear and well-defined enough to yield similar results in similar analyses so that different people will reach similar conclusions about the data.

We reviewed the approximately 51,000 records in the database as of May 2010 and the controls that exist to ensure the reliability of the data. Overall we found that controls are not adequate to ensure that the database can always be relied upon to determine the validity of a permit. Specifically, 32,000 (63 percent) of the records in the database contain inaccuracies or inconsistencies. In addition, the database is not complete, as only 55 percent of the permits issued between 2005 and 2009 are in the database. Some records had more than one type of accuracy and/or consistency problem and are listed in more than one category. We discuss these issues below.

Invalid expiration dates. More than 11,000 records (22 percent) contain inaccurate expiration dates. Specifically, the expiration dates for these records indicate that the permit was valid for more than the allowable five-year period set by statute [Section 18-12-204(1)(b), C.R.S.]. For example, we identified permit records with expiration dates indicating that the permit would not expire for 40, 50, and in some cases almost 100 years. We also found that about 18,000 records (35 percent) in the database do not have an expiration date. Without reliable expiration dates, law enforcement will not be able to determine from the database whether a permit is valid or expired.

Duplicate records. More than 2,000 records (4 percent) represent duplicate records based on the permit holder's full name (first, last, and middle name or initial). In some cases the same name appears on three, four, or five different records. As a result, law enforcement officials may not be able to determine which of these duplicate records represents the authoritative record. For example, we found 28 instances in which one of the duplicate records for a given name indicated that the individual had a valid permit while another of the duplicate records indicated that the permit had been revoked or denied.

Inconsistent records. We found about 2,700 records (5 percent) that appear to be valid permits on the initial database search screen, but are listed as not valid on a subsequent screen within the record. As noted previously, the initial screen that law enforcement agents see when they search a name in the database shows the person's name, date of birth, and whether the person has an active permit but does not show the permit's expiration date or a sheriff's notes indicating that the permit has been revoked or denied. Consequently, a law enforcement official who does not look past the initial database screen when reviewing a permit record could mistakenly assume that any of these expired, revoked, or denied records represent valid permits. This problem is significant, because law enforcement do not always look at the details behind the initial screen of a permit record. Specifically, in four interviews with local police and state trooper agencies, interviewees stated that they thought the database only contained valid permits and did not know that the database contains expired, denied, and revoked permits. Additionally, approximately 68 percent of police department and state trooper survey respondents indicated that they never or rarely go past the initial screen of a permit file to see the additional information in the permit record.

Incompleteness of database. We found that out of approximately 67,000 permits issued by sheriffs during Calendar Years 2005 through 2009, about 37,000 (55 percent) have been entered into the concealed handgun permit database. Consequently, the database does not contain records for all valid permits issued. Our analysis on completeness did not include the 14,000 permit records entered into the database before Calendar Year 2005 or after Calendar Year 2009. As noted previously, statute does not require sheriffs to enter information into the database. During Calendar Year 2009, just over two-thirds of sheriffs (44 of 64) did so. (For a chart showing the participation of sheriffs over the last five years, see Appendix A. For a map showing sheriffs who entered information into the database in Calendar Year 2009, see Appendix B.) Since the database does not contain all permit records, law enforcement cannot use the database to determine, in every instance, whether a permit is valid or invalid. For example, if an officer searches for a person's name in the database to verify whether a permit is valid and finds no record, two possibilities exist: (a) the permit is not valid, or (b) the permit is valid but the issuing sheriff did not enter the information into the database. In other words, the absence of a record in the database does not necessarily mean that a permit is invalid.

Improving the Database

As discussed above, the lack of adequate controls over the information within the database and resulting problems with data reliability limit law enforcement's ability to use the database to verify the validity of concealed handgun permits. If the General Assembly authorizes the continuation of the database beyond its sunset date of July 1, 2011, steps can be taken to improve the database. Because statute does not give CBI specific authority over the contents and operation of the database, CBI will need to work with sheriffs to implement these steps. Specifically, we identified three areas where CBI and sheriffs can take action to improve the database: (1) strengthening data integrity controls; (2) developing policies and procedures for entering, updating, and purging database records; and (3) working to correct the problematic records we identified during the audit. Other steps to improve the database would require consideration by policymakers and possible statutory change or clarification. For example, if the database continues, CBI could work with the General Assembly to establish specific authority over or responsibilities for the database. We discuss these and other considerations at the end of this report.

Data integrity controls. Databases should contain data integrity controls that help prevent a user from entering inaccurate or incomplete information in key fields. Based on our exceptions discussed above, we identified three areas in which CBI could work with sheriffs to implement stronger data integrity controls if the General Assembly decides the database should continue. First, CBI should work with sheriffs to put data integrity controls into the database so that a user cannot leave the expiration date field blank and cannot enter an inappropriate expiration date, such as a date that extends more than five years from the permit's issue date, which is beyond the time frame allowed by statute. Second, CBI and sheriffs should explore the possibility of an automated control that changes the permit record type in the database when a permit expires. This automated control would allow law enforcement to see that a permit is expired on the initial screen without searching the details of the permit record. Third, CBI and sheriffs should explore controls to minimize duplicate records in the database. For example, the database could identify when sheriffs create a record with a duplicate name and ask the sheriff to take steps to eliminate the duplicate record.

Policies and procedures for creating, updating, and removing records. Databases should have defined rules for entering or updating records and for deleting or purging expired records to keep the data relevant and reliable. As discussed above, there are inconsistencies in how sheriffs handle records. To ensure greater consistency with how concealed handgun permit information is recorded in the database if the General Assembly decides the database should continue, CBI should work with sheriffs to establish uniform policies and procedures that, at a minimum, clarify (a) how to handle denied and revoked records (i.e., whether to make notations in the record in addition to changing the record type to denied or revoked); (b) how to handle renewals (i.e., whether to create a new record and delete the old one, or update the expiration date in the existing record); and (c) when a record should be purged and who (i.e., sheriffs or CBI) has responsibility for purging old records.

Correcting problematic records. We provided the expired, duplicate, and inconsistent records we identified during the audit to CBI to correct. However, since CBI did not create the records and does not have the source data for the records, it cannot correct these. Therefore, if the General Assembly decides the database should continue, CBI should work with sheriffs to address these problematic records by cleaning up and/or purging these records to ensure that the records contained in the database are accurate and updated. For example, CBI could provide a list of inaccurate and expired records to the appropriate sheriffs for follow-up. CBI should also consider annually reviewing the database for errors and inconsistencies and providing a listing of those records to sheriffs for their review and correction.

Database Sunset

As mentioned earlier, the database will expire on July 1, 2011, if no legislative action is taken. Statute [Section 18-12-206(3)(b)(I), C.R.S.] stipulates that if the database expires, then “a sheriff shall not share information from the list of permittees with a law enforcement agency…and any law enforcement agency that receives information concerning permittees from a sheriff shall not use the information to create or maintain a statewide database of permittees. Any information concerning a permittee that is included in a statewide database…shall be removed from the database no later than July 1, 2011.” Therefore, if the General Assembly does not authorize the continuation of the database during the 2011 Legislative Session, CBI should ensure that the concealed handgun permit database and information in the database is permanently deleted and destroyed by July 1, 2011. This effort should include removing the concealed handgun permit database from the CCIC system so that law enforcement can no longer enter information into or use the database, and ensuring that permit information is not entered into other parts of the CCIC system, as occurred before 2007.

Recommendation No. 2:

If the General Assembly authorizes the continuation of the concealed handgun permit database beyond July 1, 2011, the Colorado Bureau of Investigation should improve the reliability of information in the database for determining the validity of a permit by working with sheriffs to:

a. Establish data integrity controls to help ensure that permit records are accurate.

b. Implement uniform policies and procedures for entering, updating, and purging concealed handgun permit records.

c. Address the inaccurate records identified by the Office of the State Auditor to ensure that these records contain valid expiration dates and do not contain contradictory record classification and notes, and removing records as appropriate.

d. Consider reviewing the database annually for records with errors and inconsistencies and providing a listing of those records to sheriffs for their review and correction.

Colorado Bureau of Investigation Response:

a. Agree. Implementation date: December 2011.

   If the General Assembly chooses to continue the database, CBI will work with sheriffs to (1) ensure that data entry is complete in all fields of the concealed handgun permit database with valid expiration dates for permits issued, (2) develop automated controls within the database to allow law enforcement to determine quickly the current status of a concealed handgun permit holder, and (3) improve the training of data input personnel to eliminate the incidence of duplicate records placed into the database. CBI believes that this can be accomplished during Calendar Year 2011.

b. Agree. Implementation date: December 2011.

   If the General Assembly chooses to continue the database, CBI will work with sheriffs' offices to develop appropriate policies and procedures for entering, updating, and purging concealed handgun permit records.

c. Agree. Implementation date: August 2011.

   CBI will work with sheriffs' offices to correct inaccurate records in the database identified by the Office of the State Auditor. CBI does not initiate original records so the records will be returned to the originating agencies for correction and validation.

   .

d. Agree. Implementation date: December 2011.

   CBI will work with sheriffs' offices to establish an annual review of all concealed handgun permit records contained within the database. CBI does not initiate original records so the records will be returned to the originating agencies for validation. CBI believes validations could begin in December 2011. CBI may need to seek additional funding in order to meet this requirement.

Recommendation No. 3:

If the General Assembly does not authorize the continuation of the concealed handgun permit database beyond July 1, 2011, the Colorado Bureau of Investigation should ensure that data contained in the database, including all records and information contained therein, are deleted from the Colorado Crime Information Center (CCIC) system and destroyed by July 1, 2011, pursuant to statute [Section 18-12-206(3)(b)(I), C.R.S.], and that permit information is not entered into other parts of the CCIC system.

Colorado Bureau of Investigation Response:

Agee. Implementation date: July 2011.

If the General Assembly does not authorize the continuation of the database during the 2011 Legislative Session, CBI shall ensure that the concealed handgun permit database and information in the database is permanently deleted and destroyed by July 1, 2011. This will include removing the concealed handgun permit database from the Colorado Crime Information Center (CCIC) system so that law enforcement can no longer view or enter information contained in the database.

Benefits to Law Enforcement and Public Safety

As discussed earlier, Section 2-3-118, C.R.S., requires our audit to address the benefit of the concealed handgun permit database for law enforcement and public safety in the state. During our audit we did not identify quantifiable data maintained by law enforcement agencies or other sources that could be used to assess the benefits of the database. As a result, we were not able to conclude on the benefits of the database. However, we obtained information on perceptions about the benefits of the database from law enforcement and other stakeholders through surveys and interviews as described below.

We sent 90 surveys to law enforcement agencies, including every sheriff's office, every State Trooper district, and a sample of municipal police departments. We received 74 survey responses, which represents an 82 percent response rate. Specifically, we sent surveys to and received responses from the following law enforcement agencies:

- All 64 county sheriffs' offices, with 55 responses (86 percent response rate);
- All six State Trooper districts, with four responses (67 percent response rate); and
- A sample of 20 municipal police departments, with 15 responses (75 percent response rate).

We also conducted interviews with 17 law enforcement agencies representing a variety of geographic areas across the state, including sheriffs' offices, police departments, and a State Trooper district, as well as with representatives from CBI. We also interviewed representatives from four advocacy groups, two that testified for and two that testified against House Bill 07-1174, which extended the sunset date of the database from 2007 to 2011. Finally, we accompanied law enforcement on two ride-alongs to observe how officers use the permit database during their normal duties.

Benefits to law enforcement. A total of 72 percent of survey respondents said the database benefits law enforcement, 8 percent said it does not benefit law enforcement, and 20 percent had no opinion. Three commonly cited examples of the database's benefit to law enforcement provided by survey respondents and interviewees include (a) keeping law enforcement officers safe by making them aware that a person may have a gun; (b) sharing information among law enforcement about permittees whose behavior may make them ineligible to have a permit, which can facilitate the revocation of a permit; and (c) verifying the validity of permits when a law enforcement officer comes into contact with a permittee who is carrying a concealed handgun. It is important to note that while some respondents and interviewees reported using the database to verify the validity of permits, our audit identified concerns about the reliability of the information in the database, as discussed in the previous section.

Benefits to public safety. A total of 38 percent of survey respondents said the database benefits the safety of the public, 24 percent said the database does not benefit the safety of the public, and 38 percent had no opinion. Although few survey respondents and interviewees provided specific examples of how the database benefits public safety, those who did cited the database's role in facilitating the revocation of permits of ineligible permit holders. Survey respondents and interviewees indicated that this benefits the safety of the public by (a) protecting the integrity of the concealed handgun permit process by ensuring that only eligible people have permits, and (b) making the carrying of a concealed handgun by a person whose permit has been revoked an offense upon which law enforcement may take action. Additionally, two interviewees suggested that the benefits of the database to law enforcement, described in the previous paragraph, could also be seen as benefits to public safety, since the job of law enforcement is to protect the safety of the public.

There are no recommendations in this area.

Policy Issues

While assessing the security, accuracy, and benefits of the database, we identified other possible areas for improvement of the database that the General Assembly could consider if it authorizes the continuation of the database beyond its sunset date.

Authority over the database. Policymakers may wish to consider whether CBI should be given specific statutory authority over or responsibility for the database, which could improve its reliability. As noted previously, in authorizing the database, statute [Section 18-12-206(3)(a), C.R.S.] does not name which state agency will maintain the database, and it does not charge any agency with specific duties or authority in relation to the database. Therefore, although CBI has assisted sheriffs by establishing a location for the concealed handgun permit database in CCIC, it is unclear how active CBI should be in managing the database to ensure that the data are reliable. The lack of clear assignment of oversight responsibilities for the database likely contributed to the data reliability problems we discussed previously. For example, CBI staff reported that they view the information in the database as the property of the sheriffs and have indicated that this is the reason that CBI has not created policies and procedures for standardizing the entering and updating of information into the database.

Personal information. Policymakers may wish to consider whether there should be limits or guidance on the amount of permittees' personal information that is contained in the concealed handgun permit database. As discussed previously, statute [Section 18-12-206(3)(a), C.R.S.] has outlined that the purpose of the database is to verify the validity of permits, but statute does not give guidance on what information should be contained in the database. However, statute [Section 18-12-205, C.R.S.] does outline what information can be solicited from a person when he or she applies for a concealed handgun permit. We found that sheriffs enter more personal information into the database than statute allows them to collect on the application for a concealed handgun permit. Specifically, Section 18-12-205, C.R.S., specifies that the "permit application form shall solicit only the following information from the applicant":

- Name (full name, birth name if different, and previous names if applicable);
- Date of birth;
- Address, including addresses over the last 10 years if different;
- Whether the applicant is a resident of the state; and
- Whether the applicant meets the criteria for obtaining a permit.

In contrast to the limited information that sheriffs can collect on the permit application, the database allows sheriffs to enter information into 42 different fields. As a result, sheriffs have entered significantly more personal information into the database than they are allowed to collect on the permit application. They may have collected this additional information from the background check application, the applicant's driver's license, or directly from the applicant. For example, out of the 51,000 records in the database, we found:

- 51,000 records (100 percent) contain the person's race;
- 40,000 records (78 percent) contain Social Security numbers;
- 31,000 records (61 percent) contain driver's license numbers;
- 15,000 records (29 percent) contain the person's place of birth;
- About 140 records (<1 percent) contain the person's vehicle make, color, and vehicle identification information; and
- Several records contain information about the person's occupation and place of employment.

It is unclear whether the General Assembly intended the information contained in the database to be limited to the information collected on the application. In considering whether to extend the use of the database, policymakers may wish to consider whether limits on the type of information that goes into the database are necessary.

Purpose of the database. Policymakers may wish to further clarify the ways in which the database may be used by law enforcement. Statute [Section 18-12-206(3)(a), C.R.S.] states that a "sheriff may … share information from the list of permittees with a law enforcement agency **for the purpose of determining the validity of a permit**" [emphasis added]. However, statute does not explicitly limit the use of the database only to this purpose. As discussed earlier, law enforcement officials receive information on whether an individual has been issued a concealed handgun permit whenever officials perform a general search in CCIC, regardless of whether the purpose of the search is to validate a permit. Law enforcement reported in surveys and interviews that receiving information about whether an individual may be carrying a concealed handgun is useful for promoting officer safety. According to testimony for Senate Bill 03-024, which created statewide standards for concealed handgun permits, the purpose of the database was to help law enforcement validate permits issued prior to Senate Bill 03-024, until they had all expired by June 2007. Based on our analysis of testimony for House Bill 07-1174, which extended the use of the database until July 1, 2011, we found that the rationale for the database had shifted from tracking old permits to information sharing and officer safety. However, House Bill 07-1174 did not amend the statutory purpose of the database. Therefore, policymakers may wish to consider whether the purpose and scope of the database should be clarified.

Participation by sheriffs. Policymakers may wish to consider whether requiring that all concealed handgun permits be entered into the database would make the database more accurate and reliable for law enforcement to use in determining the validity of permits. As discussed above, the database is not complete; it contains records for 55 percent of the concealed handgun permits issued from Calendar Years 2005 through 2009.

There are no recommendations in this area.

Appendices

This page intentionally left blank.

Appendix A

Colorado Concealed Handgun Permits Calendar Years 2005 Through 2009						
	2005	**2006**	**2007**	**2008**	**2009**	**Five-Year Total**
Total Permits Issued	6,300	6,200	9,400	18,000	27,000	66,900
Issued Permits Entered into the Database	3,500	3,600	6,300	8,500	15,000	36,900
Percent of Issued Permits Entered into the Database	56%	58%	67%	47%	56%	55%
Number of County Sheriffs Entering Permit Information into the Database	29	32	37	39	44	N/A
Percent of County Sheriffs Entering Permit Information into the Database[1]	45%	50%	58%	61%	69%	N/A

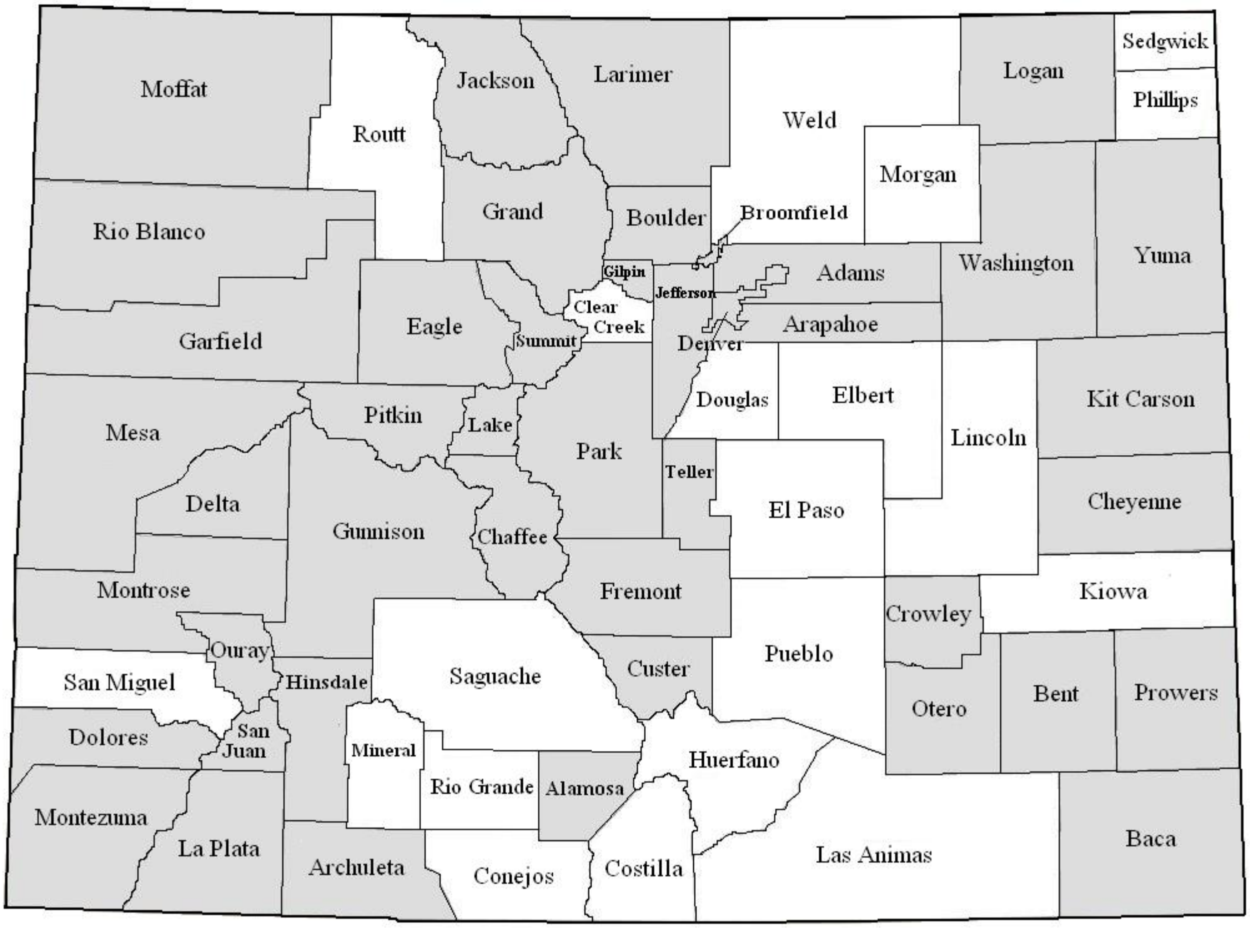
Source: Office of the State Auditor analysis of data provided by the Colorado Bureau of Investigation and County Sheriffs of Colorado annual reports to the General Assembly.

[1] There are 64 counties in the State of Colorado.

This page intentionally left blank.

Appendix B

Concealed Handgun Permit Database
Participating Counties
Calendar Year 2009



Source: Office of the State Auditor's analysis of data provided by the Colorado Bureau of Investigation.

■ 44 Counties that entered permit information into the Concealed Handgun Permit Database.

□ 20 Counties that did not enter permit information into the Concealed Handgun Permit Database.

This page intentionally left blank.

The electronic version of this report is available on the website of the
Office of the State Auditor
www.state.co.us/auditor

A bound report may be obtained by calling the
Office of the State Auditor
303.869.2800

Please refer to the Report Control Number below when requesting this report.

Report Control Number 2104

Report Control Number 2104