REPORT OF

THE

STATE AUDITOR

Public Safety Radio Communications

Performance Audit
October 2007

LEGISLATIVE AUDIT COMMITTEE
2007 MEMBERS

Senator Stephanie Takis
Chair

Representative James Kerr
Vice-Chair

Representative Dorothy Butcher
Senator Jim Isgar
Representative Rosemary Marshall
Representative Victor Mitchell
Senator Nancy Spence
Senator Jack Taylor

Office of the State Auditor Staff

Sally Symanski
State Auditor

Cindi Stetson
Deputy State Auditor

Michelle Colin
Melissa Bradley
Legislative Auditors

STATE OF COLORADO

Sally Symanski, CPA
State Auditor

OFFICE OF THE STATE AUDITOR
303.869.2800
FAX 303.869.3060

Legislative Services Building
200 East 14th Avenue
Denver, Colorado 80203-2211

October 12, 2007

Members of the Legislative Audit Committee:

This report contains the results of a performance audit of Public Safety Radio Communications. 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 24-30-908.5(6), C.R.S., which authorizes the State Auditor to review the activities of the Public Safety Communications Trust Fund. The report presents our findings, conclusions, and recommendations, and the responses of the Governor's Office of Information Technology and the Departments of Local Affairs, Personnel & Administration, and Public Safety.

This page intentionally left blank.

TABLE OF CONTENTS

This page intentionally left blank.

SALLY SYMANSKI, CPA
State Auditor

Public Safety Radio Communications
Performance Audit October 2007

Authority, Purpose, and Scope

This performance audit was conducted under the authority of Section 2-3-103, C.R.S., which authorizes the Office of the State Auditor to conduct performance audits of all departments, institutions, and agencies of state government and Section 24-30-908.5(6), C.R.S., which authorizes the Legislative Audit Committee to review the activities of the Public Safety Communications Trust Fund. The audit work was conducted from February to September 2007 in accordance with generally accepted government auditing standards. During the audit we evaluated statewide interoperability of public safety radio communications. In addition, we reviewed the Department of Personnel & Administration's management of the state-owned portion of the Digital Trunked Radio (DTR) System and the Department's controls over Public Safety Communications Trust Fund expenditures. We acknowledge the assistance and cooperation of the Departments of Personnel & Administration (DPA), Local Affairs (DOLA), and Public Safety (DPS) as well as the Governor's Office of Information Technology (OIT).

Background

"Interoperable communications" is the ability of individuals in different public safety disciplines, such as law enforcement, fire safety, and emergency medical services, and in different jurisdictions, including federal, state, and local governments, to communicate with one another through radio systems. This ability is critical for coordinating effective responses to emergencies. Interoperability can be established (1) if everyone is using the same radio system or (2) if mechanisms are in place to link different types of radio systems together. In Colorado first responders and public safety agencies use a combination of these two approaches to establish interoperability. However, the statewide DTR System is the primary communications system for many state and local agencies. The statewide DTR System, which was initially developed by DPA, is a shared trunked radio system that allows everyone who uses the System to communicate with one another, regardless of where they are located in the State. The statewide DTR System, which is owned by both the State and local governments, currently has coverage in about 86 percent of the State's geographical area. The 2006 State Homeland Security Strategy lists the DTR System as the mechanism the State will use to achieve interoperability.

Overall, almost $135 million in state-directed funds has been allocated to state agencies and local governments to improve interoperable communications in Colorado. This includes about $84 million in state and federal grants and about $51 million in state capital construction funds. The state capital construction funds were appropriated to the Public Safety Communications Trust Fund, which is administered by DPA.

Summary of Audit Findings

Statewide Interoperability

We reviewed Colorado's progress in achieving statewide interoperability, as set forth in state statutes, federal goals and grant requirements, and the State Homeland Security Strategy. Specifically, we assessed (1) the availability of data necessary to evaluate statewide communications capabilities, system usage, and needs; (2) how DOLA targets funds to further statewide interoperability and address risk; and (3) the State's strategic approach to achieving interoperability. We identified the following issues:

- **Data for Assessing Interoperability.** Although there are indications that the State has made progress in achieving statewide interoperability, we found that the fundamental data are lacking to determine specifically how much progress has been made. According to self-assessment data prepared by the nine all-hazards emergency management regions across the State and submitted to DOLA in October 2006, most regions have made "initial efforts" or "moderate progress" toward achieving interoperability. Although these data indicate that the State still has some serious deficiencies in attaining interoperable communications, the limited data are not complete or sufficient to assess the extent to which statewide interoperability has been achieved, identify gaps in capabilities, or determine and quantify the resources needed for the State to become fully interoperable.

- **Targeting Funds.** We reviewed DOLA's distribution of grant funds to the nine all-hazards emergency management regions from 2004 through 2006 and found that DOLA did not prioritize statewide interoperable communications needs on the basis of risk when making these grant distributions. Additionally, we found that DOLA did not have a systematic method for evaluating specific funding requests for interoperable communications projects against statewide interoperable communications needs and priorities.

- **Statewide Strategic Approach.** We reviewed the State's approach to achieving statewide interoperability and found that the State has not taken a coordinated and strategic approach to communications planning. OIT should work with the General Assembly, as needed, to create a governing body for coordinating statewide interoperable communications and assigning responsibilities to this body. Once established, the governing body should work with DOLA, DPA, and DPS to establish a statewide strategic approach for planning and implementing statewide interoperable communications and for targeting dollars effectively.

Digital Trunked Radio System

We reviewed DPA's oversight of the state-owned portion of the DTR System and its administration of the Public Safety Communications Trust Fund (the Fund) and identified the following issues:

- **CCNC Participation.** We reviewed the statutes and determined that it is unclear whether DPA has authority to participate in the Consolidated Communications Network of Colorado (CCNC) under current law. The CCNC is a public nonprofit corporation that exists to "assist in the development of facilities, operational procedures, maintenance, grants, and training for the statewide digital trunked radio network." Participation in the CCNC, without the explicit approval of the General Assembly, may present risks to the State.

- **Disaster Recovery Planning.** We found DPA may not be adequately testing its disaster recovery plan as required by the Chief Information Security Officer's (CISO's) disaster recovery policy. We also found that DPA needs to document all required procedures in its disaster recovery plan and maintain the plan, including updating the plan on a quarterly basis, as required by the CISO's disaster recovery policy.

- **System Training.** We reviewed DPA's training records for the State's two zone controller engineers and 13 of the State's 28 transmitter site technicians and found that none of the 15 engineers and technicians has completed all of the CCNC's minimum training requirements.

- **Capital Assets.** We found that DPA cannot substantiate the basis for capitalizing repair and maintenance costs or the estimated useful life used in capitalizing these expenditures for the DTR System. Additionally, we found that state and federal guidelines suggest that 15 years may not be an appropriate useful life for all components of the DTR System.

- **Radio Inventory.** We found that DPA is conducting its annual physical inventory of all state-owned digital trunked radios after fiscal year end and recording any necessary adjustments to capital assets in the accounting records for the following fiscal year.

- **Controls Over Disbursements.** We found that 3 of the 19 payment vouchers we reviewed did not have the required approval documented by DPA finance staff. Although our review did not identify any payment errors, documented approval prior to payment is an important control for ensuring payments are accurate.

Our recommendations and the responses of the Governor's Office of Information Technology and the Departments of Local Affairs, Personnel & Administration, and Public Safety can be found in the Recommendation Locator and in the body of the report.

This page intentionally left blank.

RECOMMENDATION LOCATOR

Rec. No.	Page No.	Recommendation Summary	Agency Addressed	Agency Response	Implementation Date
1	27	Implement mechanisms to collect reliable and sufficient data on the State's current communications capabilities and needs and the resources required to achieve statewide interoperability.	Department of Local Affairs	Agree	June 2008
2	30	Improve practices for evaluating communications capabilities, needs, and risks; ensure these evaluations consider risks and priorities from a statewide perspective; and target grant funds toward communication projects that address the State's greatest risks, needs, and any other relevant factors and result in measurable improvements to statewide interoperability.	Department of Local Affairs	Agree	June 2008
3	33	Work with the General Assembly, as needed, to evaluate options for establishing a governing body that is responsible for coordinating statewide interoperable communications, establish a strategic approach for planning and implementing statewide interoperable communications and for targeting funds to strengthen communications capabilities, and maintain and update the statewide interoperable communications plan.	Office of Information Technology	Agree	July 2008
			Department of Local Affairs	Agree	June 2008
			Department of Personnel & Administration	Agree	June 2008
			Department of Public Safety	Agree	July 2008
4	44	Seek a legal opinion from the Attorney General's Office to determine whether the Department is statutorily authorized to participate in the Consolidated Communications Network of Colorado and work with local governments to evaluate alternatives for managing the statewide Digital Trunked Radio System.	Department of Personnel & Administration	Agree	June 2008

RECOMMENDATION LOCATOR

Rec. No.	Page No.	Recommendation Summary	Agency Addressed	Agency Response	Implementation Date
5	47	Develop and maintain a current and comprehensive disaster recovery plan for the statewide Digital Trunked Radio System, including the state- and locally-owned portions of the System, and conduct tabletop exercises under simulated emergency conditions.	Department of Personnel & Administration	Agree	June 2008
6	50	Ensure staff responsible for maintaining the Digital Trunked Radio System receive the appropriate and necessary training by reviewing the appropriateness of current minimum training requirements, identifying alternatives for employees to receive the necessary training, and considering exempting employees from training requirements if the employees are proficient in the subject matter.	Department of Personnel & Administration	Agree	June 2008
7	53	Establish procedures for ensuring all repair and maintenance costs are analyzed and classified in accordance with the Fiscal Procedures Manual; review the appropriateness of the estimated 15-year useful life used for depreciating components of the Digital Trunked Radio System; and adjust, as necessary, the State's accounting records.	Department of Personnel & Administration	Agree	November 2008
8	56	Conduct the physical inventory of Digital Trunked Radio System radios and adjust capital assets before the end of the fiscal year, continue to work with state agencies to improve cooperation with the Department's physical inventory process, and consider upgrades to the System's reporting capabilities.	Department of Personnel & Administration	Agree	July 2008
9	58	Ensure all invoices are reviewed and approved by the Department's finance office prior to authorizing vendor payments.	Department of Personnel & Administration	Agree	Implemented

Description of Public Safety Radio Communications

Background

Every day first responders to emergencies across the nation rely on public safety radio communications systems to communicate with one another during events ranging from routine traffic accidents to national emergencies or disasters, such as Hurricane Katrina and the terrorist attacks on September 11, 2001. First responders are public safety agencies, such as law enforcement, fire safety, and emergency medical services, that receive the initial calls to respond when emergencies occur. The ability of first responders to use radio systems to communicate within and across different agencies or disciplines and jurisdictions is called interoperability, or interoperable communications. The U.S. Department of Homeland Security lists strengthening interoperable communications among first responders as one of the nation's top priorities. Additionally, the Colorado General Assembly recognized in statute (Section 24-30-901, C.R.S.) that:

> An essential component of a viable telecommunications policy is the availability of a statewide, interoperable public safety radio communications system that provides instant and disruption-resistant communication capability for law enforcement agencies and other units of government that may be called upon to deal with natural disasters, health emergencies, acts of terrorism, and other threats to public health and safety.

This report focuses on two aspects of interoperable communications:

- Statewide interoperability, which addresses the State's progress in developing statewide interoperable communications and is discussed in Chapter 1, and

- The state-owned portion of the Digital Trunked Radio System (explained later in this Description Chapter), which addresses the Department of Personnel & Administration's management of the System and the Public Safety Communications Trust Fund and is discussed in Chapter 2.

Below we describe the technology supporting interoperable communications in a public safety environment and oversight responsibilities with respect to interoperable communications. We also provide a brief description of the Digital Trunked Radio

System, which is a key component of establishing interoperable communications statewide.

Public Safety Radio Systems

Public safety radio systems typically operate by transmitting voice communications from one user through radio frequencies, or channels, to a radio transmitter tower that sends the message to another user who is on the same frequency. There are basically two different types of public safety radio systems—conventional systems and shared trunked systems. Conventional and shared trunked radio systems differ in how radio frequencies are assigned to users and how radio towers are used to transmit communications. In a conventional radio system, communications are limited to users who are on the same frequency, or channel, and who are within a certain distance of each other and the same radio tower. Users who routinely communicate with one another, such as a police department or fire department, are assigned a specific frequency to use. In a conventional system, users must physically select on their radios the frequency that they want to use and monitor.

A shared trunked radio system is more complex than a conventional system. A shared trunked system uses talk groups and microprocessors called zone controllers to assign frequencies to users on an as-needed basis. Each radio is programmed with different talk groups to address the user's communications needs. A talk group is a defined group of users that need to be able to communicate with one another, such as a fire department or a police department. When a "call" is initiated by a user within a talk group, the system uses a zone controller to automatically assign a frequency to the talk group. By assigning frequencies as they are needed, shared trunked systems allow a large number of talk groups to share a small number of frequencies. Additionally, in a shared trunked system, radio towers can be configured to allow members of the same talk group to communicate with one another, even though they may not be within the coverage area of the same radio tower. Colorado's Digital Trunked Radio (DTR) System, as discussed later in this Chapter and in Chapter 2, is a shared trunked system. From an interoperability perspective, shared trunked radio systems are optimal because they facilitate communications among first responders during emergencies that affect a larger area and require responses from numerous public safety agencies. In essence, if a first responder has a radio that operates on a shared trunked system, the first responder can talk to anyone else on that shared trunked system; no additional connection device or hardware is required.

If first responder agencies use different types of radio systems (e.g., two or more different conventional or shared trunked systems or both conventional and shared trunked systems), there are still ways to establish interoperability, including:

- **Gateway devices,** which allow agencies to link two or more radio systems that are otherwise incompatible. When a gateway device is in place, users from the different systems can communicate with one another even though they are not on the same frequencies. In most cases, someone must physically connect the gateway device to the different systems for the users to be able to communicate.

- **Radio caches,** which are extra radios maintained in deployment-ready condition to be distributed to first responders during an incident. For example, a police department will have extra radios on hand that it will give to someone from the fire department when an emergency occurs. These radios will be programmed with the same frequencies as those used by the police department and thus, will allow the fire department to communicate with the police department during the emergency. Once the emergency is over, the police department would take the radios back and have them on hand for future emergencies.

- **Shared frequencies,** which in some instances can be programmed into radios from different systems to allow the users to communicate with one another. Shared frequencies are an option when agencies' radio systems operate in the same radio band. For example, first responder agencies using two different conventional VHF radio systems, both operating in the 150 to 160 Megahertz (MHz) frequency band, can program their radios with a set of common radio frequencies so that they can communicate with each other during an emergency.

When first responders have to use gateway devices, radio caches, or establish shared frequencies to communicate with one another, this can be more difficult and often takes time to arrange during an emergency.

State Oversight

In Colorado, three state departments, the Governor's Office of Information Technology, the nine all-hazards emergency management regions, and the Consolidated Communications Network of Colorado have important roles in planning and implementing interoperable communications across the State. Specific responsibilities of all these parties include:

- **Department of Personnel & Administration (DPA).** According to the statute (Section 24-30-903, C.R.S.), DPA is responsible for current and long-range telecommunications planning for state government. This includes keeping informed of changes in technology and making recommendations for

improving state telecommunications systems, including the State's public safety radio system. The statute also requires DPA to establish telecommunications procedures and standards for all state agencies. As part of its telecommunications responsibilities for state government, Senate Bill 91-227 directed DPA to work with the Colorado State Patrol to develop a plan to replace and update the State's existing public safety radio system. DPA developed the plan for the DTR System in 1995, as discussed later in this chapter. The Division of Information Technologies within DPA is responsible for overseeing and maintaining the state-owned portion of the DTR System. The Division of Information Technologies also works with the Consolidated Communications Network of Colorado (CCNC), as discussed later in this section, to collaborate with local and federal DTR System users with respect to expanding and maintaining the statewide DTR System. Pursuant to a memorandum of understanding (MOU) established in June 2007 between DPA and the Governor's Office of Information Technology (OIT), the Division of Information Technologies, although organizationally within DPA, is now under the operational management of OIT.

- **Department of Local Affairs (DOLA).** The Division of Emergency Management within DOLA is responsible for administering the federal Homeland Security Grant Program that has provided more than $44 million to state agencies, including DPA, DOLA, the Department of Public Safety (DPS), and the Department of Natural Resources (DNR), and to local governments to improve interoperable communications. Specifically, the Division of Emergency Management is responsible for reviewing applications for Homeland Security Grants and determining how the grant dollars will be distributed to state agencies and local jurisdictions. Additionally, the Division of Emergency Management is required by the Homeland Security Grant Program and state statute (Section 24-32-2116(2), C.R.S.) to adopt and maintain a tactical and long-term statewide interoperable communications plan that addresses how first responders across the State will link their radio systems to establish communications during an inter-disciplinary and/or inter-jurisdictional emergency. The Division of Local Government, also within DOLA, is responsible for administering the Colorado Wireless Interoperability Network (CWIN) Initiative, a one-time initiative which was created by DOLA and funded with the State's Energy and Mineral Impact Grants, to expand the DTR System. (Note: Energy and Mineral Impact Grants are funded by a portion of the State's severance tax revenue and revenue from federal mineral leases.) In 2005 and 2006 the Division of Local Government distributed approximately $35 million in CWIN funds to local governments to purchase infrastructure for the DTR System.

- **Department of Public Safety (DPS).** The Office of Preparedness, Security, and Fire Safety within DPS is responsible for investigating terrorist threats in Colorado and assessing the State's preparedness to respond to those threats, which includes the ability of first responders to communicate during an emergency. As part of this responsibility, DPS must assess and maintain data on statewide risks and vulnerabilities and identify the State's critical infrastructure. Statewide risks, vulnerabilities, and critical infrastructure are all factors that should be considered when planning and funding interoperable communications.

- **Governor's Office of Information Technology (OIT).** OIT is responsible for improving the efficiency of state government by overseeing information technology initiatives, including the DTR System under the June 2007 MOU with DPA mentioned earlier. According to the statute (Section 24-37.5-108, C.R.S.); this includes reviewing the statewide communications and information infrastructure to make recommendations on requirements and use of the infrastructure; to determine where infrastructure exists and if the existing infrastructure meets present and future user needs; and to advise state agencies about any risks, issues, and concerns related to the infrastructure. In addition, OIT's mission and objectives include securing and protecting existing information technologies; managing and optimizing spending for information technology projects; and improving service delivery, collaboration, and innovation.

- **Colorado's Nine All-Hazards Emergency Management Regions and the Denver Urban Area Security Initiative (UASI).** The nine all-hazards regions were established through Executive Order D 013 03 issued in July 2003 to help facilitate emergency management and response collaboration and planning across the State. Additionally, the Denver metropolitan area UASI, which is located in the North Central region, was designated by the U.S. Department of Homeland Security as an area considered to be of high-threat and high-density and thus, eligible to receive additional federal Homeland Security Grant funds known as the UASI grants. The local governments within each region are required to coordinate with one another to prepare and submit Homeland Security Grant applications to DOLA. The statute (Section 24-32-2116(3), C.R.S.) also requires each region to adopt a tactical and long-term interoperable communications plan that addresses how first responders in the region will link their radio systems to establish communications during an emergency. The regions were required to submit their regional plans to DOLA by November 1, 2006. DOLA is responsible for using the regional plans when preparing the State's tactical and long-term interoperable communications plan required by the federal Homeland Security Grant Program and state statute. The State's plan is due to the

federal government by the end of Calendar Year 2007. The following map shows the nine regions.

State of Colorado
All-Hazards Regions
September 2007

Source: Department of Local Affairs.

- **Consolidated Communications Network of Colorado (CCNC).** The CCNC is a public nonprofit corporation that exists to "assist in the development of facilities, operational procedures, maintenance, grants, and training for the statewide digital trunked radio network." The CCNC was created by an employee of a participating local government in 2002 to address operational issues and to facilitate cooperation among state, local, and federal agencies that share ownership and/or use of the statewide DTR System. The CCNC has established standard operating procedures and a service level agreement for promoting the cooperative use and maintenance of the System. To join the statewide DTR System, user agencies must become members of the CCNC. The CCNC is governed by a 36-member Board of Directors elected by user agencies and an 11-member Executive Directors Committee elected by the Board of Directors. As of September 2007, the CCNC had about 700 members. The State, represented by DPA, is

one of the members and holds a permanent seat on the Executive Directors Committee. The CCNC is discussed in more detail in Chapter 2.

Digital Trunked Radio System

The DTR System is used by both state and local government agencies and is a key component of statewide interoperability. The DTR System is a shared trunked radio system initially developed by DPA to improve interoperable communications capabilities for state agencies, in particular the Colorado State Patrol. DPA began planning the DTR System about 15 years ago as a result of Senate Bill 91-227 and the November 1991 *Division of Telecommunications Performance Audit* conducted by the Office of the State Auditor, which both recognized that the State's conventional radio systems were antiquated and needed to be updated.

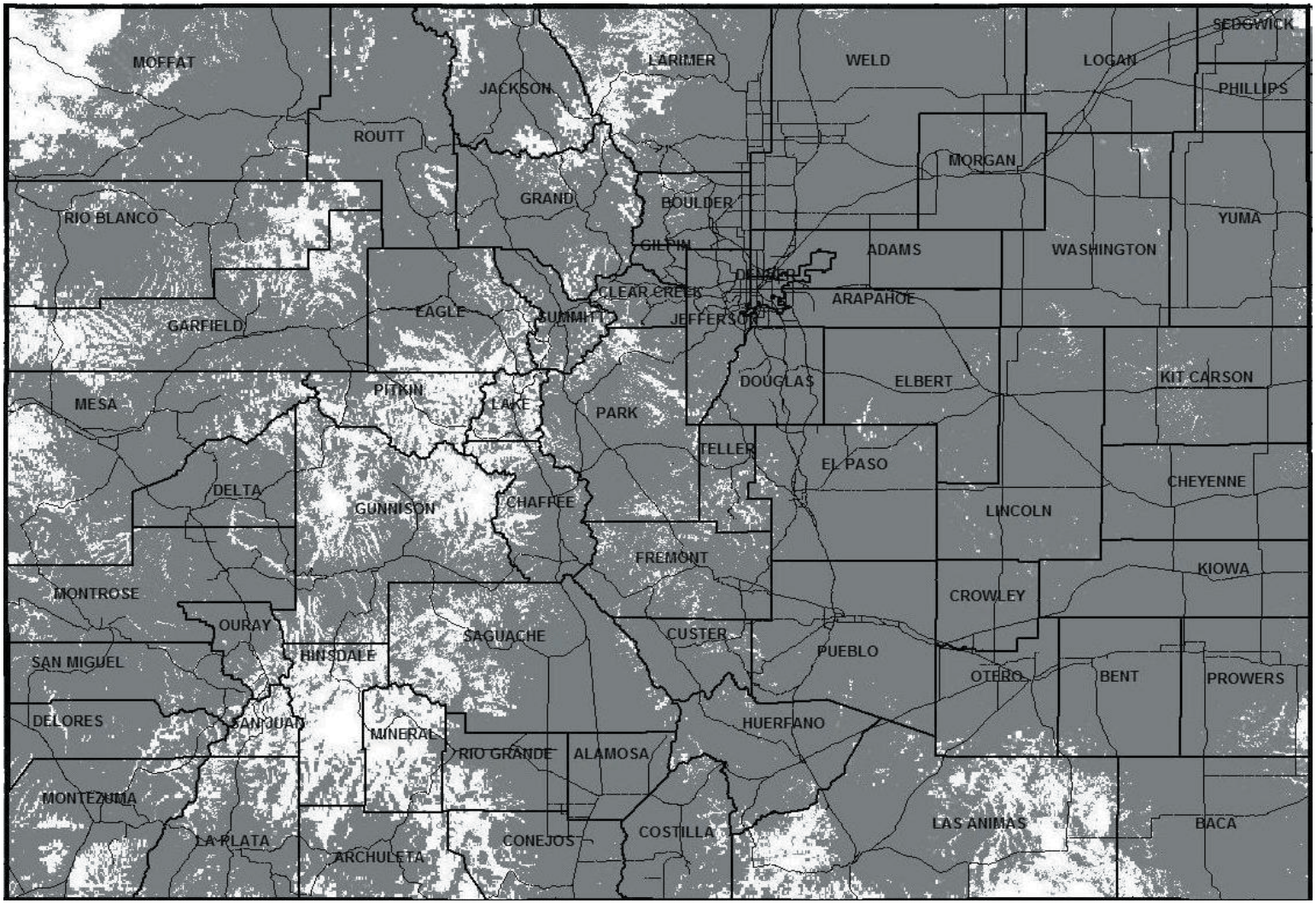
In 1998, prior to when DPA began the implementation of the DTR System, the General Assembly recognized in the statute (Section 24-30-903, C.R.S.) the need to develop an interoperable public safety radio system that was not limited to only state agencies but also included local and federal agencies. To this end, the statute directed DPA's Executive Director to carry out duties and responsibilities related to the State's public safety radio communications systems "in a manner that is consistent with the objective of maximizing access to digital networks of the State by all public offices of all levels, branches, and political subdivisions of the State within every community of the State." DPA has worked with local and federal agencies in developing the DTR System as required by the statute. As a result, the DTR System is designed to handle a large number of users from across the State, and local and federal agencies can easily join the System as long as they have compatible digital radios and are within System coverage areas. Additionally, due to a lack of available funding at the state level, many local governments have used their own funds, including state and federal grant funds, to help build the DTR System infrastructure. As the following table shows, local governments currently own a significant portion of the DTR System.

Statewide Digital Trunked Radio System Infrastructure Ownership as of September 2007			
Infrastructure	**State-Owned**	**Locally Owned**	**Total**
Zone Controllers	2	1	3
Radio Towers	78	66	144
Source: Department of Personnel & Administration data.			

In this report, we refer to the "statewide DTR System" when discussing the entire Digital Trunked Radio System, including both state- and locally-owned components. We refer to the "state-owned portion of the DTR System" when discussing the portions of the Digital Trunked Radio System owned by the State and managed by DPA. As noted previously, we discuss interoperable communications and the statewide DTR System in Chapter 1 and the state-owned portion of the DTR System in Chapter 2.

Currently the statewide DTR System has coverage in about 86 percent of the State's geographical area. According to DOLA, there are about 100 state and local dispatch centers in Colorado. Dispatch centers coordinate the day-to-day radio communications for public safety agencies. A single dispatch center often serves multiple public safety disciplines within a jurisdiction, such as the police, fire safety, and emergency medical services in a county. In some cases, there is one dispatch center that provides dispatch services for all of the public safety agencies in several jurisdictions. Approximately half of the 100 dispatch centers use the statewide DTR System on a regular basis as their primary communications system. This includes about 30 dispatch centers that solely use the statewide DTR System and about 20 dispatch centers that use the statewide DTR System in conjunction with other systems. According to DPA, local governments plan to build another 24 radio transmitter towers for the statewide DTR System by the end of 2007 and 10 more towers in 2008, using primarily CWIN grant funds from DOLA. With the installation of these 34 radio towers, statewide coverage will increase to 94 percent and all state agencies will have System coverage. As discussed in Chapter 1, although the DTR System is available throughout most of the State, local agencies can only use the System if they have digital radios that are compatible with the System. Additionally, the State and local governments have the option of installing additional towers to increase statewide coverage to 100 percent. The following map shows DTR System coverage as of September 2007.

Digital Trunked Radio (DTR) System
System Coverage as of September 14, 2007



Source: Department of Personnel & Administration.
Note: Coverage Area is shaded.

Fiscal Overview

Colorado's investment in interoperable communications has been financed through several different funding sources. This includes state capital construction funds, which have been used to help implement the state-owned portion of the DTR System, and federal Homeland Security Grant funds and state CWIN grant funds, which have been used to implement the statewide DTR System and other communications projects. As shown in the following table, almost $135 million in state-directed funds has been allocated to state agencies and local governments to improve interoperable communications in Colorado.

State-Directed Funding Allocations for Interoperable Communications
Fiscal Years 1999 Through 2007
(In Millions)

Agency	Funding Source				
	State Capital Construction[1]	Homeland Security Grants[2]	CWIN Initiative	Other Federal Grants[3]	Total
Personnel & Administration	$51.0	$1.2	$0	$4.5[4]	$56.7
Local Affairs	$0	$1.7	$0	—	$1.7
Public Safety	$0	$0.2	$0	—	$0.2
Natural Resources	$0	$0.6	$0	—	$0.6
Local Governments	$0	$40.7	$34.7	—	$75.4
Total	**$51.0**	**$44.4**	**$34.7**	**$4.5**	**$134.6**

Source: Office of the State Auditor's analysis of data provided by DOLA and DPA.

[1] Capital construction funds includes interest income on the Public Safety Communications Trust Fund.

[2] 2004 through 2006 Homeland Security Grants. This includes about $11 million allocated to the Denver metropolitan area through the Urban Area Security Initiative.

[3] In addition to the $4.5 million, the Departments of Local Affairs, Public Safety, and Natural Resources and local governments may have received other federal grants for improving interoperable communications that are not reflected in this table.

[4] Includes about $2.9 million from other Homeland Security Grants, $1.0 million from the Community Oriented Policing Services (COPS) 2003 Technology Grant, $500,000 from the U.S. Office of Justice Programs, and $84,000 from the Chemical Stockpile Emergency Preparedness Program.

Audit Scope and Methodology

This audit reviewed the planning and implementation of statewide interoperability, including evaluating the role of the statewide DTR System in improving statewide interoperable communications. Additionally, the audit reviewed DPA's administration of the state-owned portion of the DTR System and DPA's controls over Public Safety Communications Trust Fund (Fund) expenditures. The Legislative Audit Committee (Committee) is statutorily required to review expenditures from the Fund every two years (Section 24-30-908.5(6), C.R.S.). Our Office last reported to the Committee on the Fund in June 2005. As part of our audit work, we reviewed statutory requirements, analyzed data, and interviewed DPA, DOLA, and DPS staff, regional coordinators, CCNC staff, and local dispatch centers. We also contacted five other states (Arizona, Montana, New Mexico, Utah, and Wyoming) regarding their public safety radio systems.

This page intentionally left blank.

Statewide Interoperability

Chapter 1

Background

"Interoperable communications" is the ability of individuals in different public safety disciplines, such as law enforcement, fire safety, and emergency medical services, and in different jurisdictions, including federal, state, and local governments, to communicate with one another through radio systems. Interoperable communications is critical to the ability to respond to all types of emergencies and disasters. Events, such as Hurricane Katrina and the terrorist attacks of September 11, 2001, have shown how important it is that first responders be able to communicate with one another when an emergency or a disaster occurs.

There are essentially two ways to establish interoperability across disciplines and jurisdictions. The first and easiest way is to have everyone use the same radio system. Shared trunked systems, such as the Digital Trunked Radio (DTR) System, allow users from all across the State to share frequencies, or channels, and communicate with one another regardless of location, as long as coverage is available. Interoperability can be quickly and easily achieved if everyone is on the same shared trunked system because the users only need to select a common talk group on their radio and the system automatically assigns a channel. The second way to establish interoperability can be more difficult and is used when everyone is not on the same system. It requires implementing mechanisms or devices to link different types of systems together. For example, there are gateway devices that can be used to link a conventional system with another conventional system and/or with the DTR System or another shared trunked system. Linking two systems, however, may require obtaining a radio from each different system and physically connecting the radios with one or more gateway devices. Thus, unlike a shared trunked system, such as the DTR System, establishing communications through a gateway device is not instantaneous and, in an emergency, critical time may be lost.

The first responders and public safety agencies in Colorado use a combination of these two approaches (shared trunked systems and linking devices) to establish interoperability. As discussed previously, many state and local agencies use the DTR System as their primary communications system. These agencies have shared channels and can talk with one another at any time, as long as they are located in an area with DTR System coverage. The DTR System, however, is just one piece of the State's interoperable capabilities. There are still state and local agencies that

continue to use either conventional systems or shared trunked systems other than the DTR System as their primary communications systems. As discussed in the Description Chapter, DTR System coverage has not been fully implemented in some western portions of the State due to funding limitations. Therefore, the DTR System is not an option at this time for state and local agencies in these areas; they must continue to use conventional radio systems or other shared trunked systems. Additionally, some local agencies have continued to use other radio systems, even though the DTR System is available in their areas. According to DPA, some of the reasons local agencies are not using the DTR System include a lack of funding to purchase digital radios or prior investments in different types of radio systems.

This report discusses two aspects of the State's public safety communications capabilities. In this chapter we review statewide progress in developing interoperable communications, which is the ability of first responders to talk with one another when needed. In Chapter 2 we discuss DPA's management of the state-owned portion of the DTR System. Both chapters recommend ways to help improve statewide interoperable communications and to ensure that state-directed dollars are used effectively and accounted for appropriately.

Interoperability

According to the U.S. Department of Homeland Security, strengthening interoperable communications is a national priority. Colorado has also recognized the importance of interoperability. In 1998, before the events of September 11 or Hurricane Katrina, the General Assembly established in the statute (Section 24-30-901, C.R.S.) that "an essential component of a viable telecommunications policy is the availability of a statewide, interoperable public safety radio communications system . . . ."

Additionally, Colorado's State Homeland Security Strategies for 2003 through 2006, developed by the Department of Local Affairs (DOLA) and the Department of Public Safety (DPS), included strengthening interoperable communications capabilities and achieving statewide interoperability as top priorities. According to the 2006 State Strategy, Colorado intends to achieve statewide interoperability by (1) expanding the DTR System and (2) maintaining a statewide operational plan for interoperable communications. Further, the U.S. Department of Homeland Security requires states receiving Homeland Security Grant funds to assess their current communications capabilities, target grant funding to improve interoperability in areas with the greatest risks and needs, and conduct statewide planning to improve interoperable communications.

As explained in the Description Chapter, to date Colorado has allocated about $135 million in state-directed funds, in addition to funds contributed by local governments, to improve statewide interoperable communications. We reviewed Colorado's progress in achieving statewide interoperability, as set forth in state statutes, federal goals and grant requirements, and the State Homeland Security Strategy. Specifically, we assessed (1) the availability of data necessary to evaluate statewide communications capabilities, system usage, and needs; (2) how DOLA targets funds to further statewide interoperability and address risk; and (3) the State's strategic approach to achieving interoperability. We discuss our findings in each of these areas below.

Data for Assessing Interoperability

The General Assembly, through the statute (Section 24-32-2116, C.R.S.), and the U.S. Department of Homeland Security, through grant provisions, require DOLA to prepare a statewide interoperable communications plan. According to state and federal requirements, this plan is to include (1) a state strategy for improving statewide interoperability; (2) an assessment of the State's current communications capabilities; (3) provisions for funding or identifying funding sources that can be used to improve and sustain interoperable communications; (4) plans for a statewide training, testing, and exercise program; and (5) tactical procedures for establishing interoperability. To prepare this plan, DOLA must have comprehensive data on the State's current communications capabilities, any gaps in those capabilities, and the additional capabilities and resources needed for the State to achieve interoperability.

We reviewed the information available on statewide communications capabilities and needs to assess the extent to which statewide interoperability has been achieved. Overall, we found that there are indications that progress has been made in achieving statewide interoperability since 1998. As noted previously, DPA data indicate that the statewide DTR System currently has coverage in 86 percent of the State. Additionally, staff report that state and local agencies were able to use the System successfully to communicate with one another during recent state emergencies, including the Holly tornado. However, we found that the fundamental data are lacking to fully determine how much progress has been made in achieving statewide interoperability. Additionally, the limited data that are available are not complete or sufficient to assess the extent to which statewide interoperability has been achieved, identify gaps in capabilities, or determine and quantify the resources needed to become fully interoperable. Specifically, at the time of our audit, DOLA did not have comprehensive statewide information on (1) the total number of public safety and first responder agencies in the State; (2) the types of communications systems used by the public safety and first responder agencies; (3) which public safety and first responder agencies need to communicate with one another, either within or

outside of their own jurisdiction, and whether they are able to adequately establish communications for routine operations or in the event of an emergency; (4) the number of digital trunked radios, gateway devices, or other equipment needed by local public safety and first responder agencies to become fully interoperable statewide; or (5) the need for additional training, testing, and exercising to effectively operate the communications systems that are in place during an emergency. We discuss the data issues we found related to assessing statewide communications capabilities, systems usage, and needs in the following sections.

Communications Capabilities

To achieve statewide interoperability, the State must first identify its current communications capabilities and determine where the State's interoperable capabilities are lacking. To this end, the U.S. Department of Homeland Security has required each state to submit a statewide interoperable communications plan by the end of Calendar Year 2007 as a condition of receiving 2006 and 2007 Homeland Security Grants, as well as to qualify for federal Public Safety Interoperable Communications Grant funds. The statewide plan is to include, among other things, an assessment of the State's current communications capabilities.

To assess the State's progress in achieving statewide interoperability, we first reviewed information on statewide communications capabilities prepared by the nine all-hazards regions and submitted to DOLA in October 2006. DOLA asked each of the nine regions to self-assess its overall communications capabilities against 16 measures (listed in the Appendix). We found that the regional self-assessments were not based on quantifiable, verifiable data, and the information provided through the assessments was not sufficient to comprehensively assess statewide communications capabilities and identify gaps.

The self-assessment measures were meant to provide information on the extent to which each region had communications systems in place that would allow public safety and first responder agencies in the regions to communicate with other public safety and first responder agencies when necessary. For example, each region was asked to assess the extent to which interoperable communications in the region exists (1) across disciplines, (2) across jurisdictions, (3) between the State and local governments, and (4) with federal government responders with which first responders in the State need to communicate.

We evaluated the information reported by the nine regions and found that none of the regions reported they had achieved full communications capabilities as defined by the 16 measures. The following table shows the average capability rating reported by each region. As the table shows, on a scale of "0" (low) to "5" (high), the average ratings ranged from 2.3 to 3.6, which means that, overall, the regions reported that

they are either in the "initial efforts" or have made "moderate progress" toward achieving interoperability.

Department of Local Affairs
Homeland Security Grant Program
Self-Assessed Communications Capabilities
Nine All-Hazards Regions
October 2006

Region [1]	Communications Capabilities Rating[2] (based on a rating scale of 0 to 5)
1	2.3
2	2.6
3	2.6
4	2.8
5	3.1
6	3.1
7	3.1
8	3.3
9	3.6

Source: Office of the State Auditor's analysis of capabilities data collected by the Center for the Study and Prevention of Violence at the University of Colorado at Boulder on behalf of the Department of Local Affairs.

[1] A random identifying number has been assigned to each region for confidentiality purposes.

[2] The regions were asked to rate their communications capabilities for each of 16 measures according to the following scale: (0) "no recognition of need," (1) "recognition of need," (2) "initial efforts," (3) "moderate progress," (4) "sustained efforts," or (5) "output achieved." These measures, located in the Appendix, assessed the extent to which the region had communications systems in place that would allow public safety and first responder agencies in the region to communicate with other public safety and first responder agencies.

Overall, there were certain communications capabilities that received particularly low ratings by most of the regions. For example, of the nine regions:

- Eight reported a score of 2 ("initial efforts") or less when assessing their progress toward achieving interoperable communications with federal government first responders.

- Six reported a score of 2 ("initial efforts") or less when assessing their progress in establishing interoperability solutions for all first responders that do not require intervention by a third party (e.g., a dispatcher does not have to physically patch two or more systems together).

- Five reported a score of 2 ("initial efforts") or less when assessing whether they regularly test or exercise their plans, procedures, and use of interoperable communications equipment.

These ratings indicate that there are still some serious deficiencies in self-assessed statewide communications capabilities. However, there were no baseline data with which to compare the results of the regional self-assessments to determine how much statewide communications capabilities have improved since 1998, after investing approximately $135 million in state-directed funds in interoperable communications. Additionally, since DOLA did not require the regions to provide quantifiable data to support their assessments, the self-assessments cannot be used to systematically identify the additional needs and resources for addressing those gaps. As a result, the regional self-assessments have limited value in identifying improvements needed to attain interoperable communications or directing additional funding. Therefore, the State may not be able to rely on the self-assessments as an accurate representation of the regions' communications capabilities to respond effectively to a disaster.

Communications Systems Usage

Our second approach in attempting to assess statewide interoperable capabilities was to work with DOLA in an effort to obtain an inventory of the public safety and first responder agencies in the State, identify the types of communications systems used by these agencies, and determine the extent to which these agencies use the statewide DTR System as one of their primary communications systems. As discussed previously, the State Homeland Security Strategy specifically states that expanding the DTR System is a primary mechanism for achieving interoperability. We found that DOLA does not maintain sufficient information to comprehensively identify a complete inventory of the public safety and first responder agencies in the State or the types of communications systems these agencies are using. Further, we found that there are no standard definitions to consistently identify the state and local public safety and first responder agencies.

During the audit DOLA began collecting data on the public safety and first responder agencies in the State at our request. According to the information reported by DOLA, there are approximately 700 public safety and first responder agencies in the State. Of these, DOLA reports about 300 use the statewide DTR System as their primary communications system, another 300 use conventional systems as their

primary communications systems, and about 100 use shared trunked systems other than the statewide DTR System as their primary communications systems. However, we found that the information collected by DOLA is not consistent with information provided by DPA on DTR System users. As the agency responsible for overseeing the state-owned portion of the DTR System, DPA maintains information on DTR System user agencies. According to DPA and the Consolidated Communications Network of Colorado (CCNC), as of September 2007, there were about 500 public safety and first responder agencies using the statewide DTR System as their primary communications system. DPA and the CCNC did not have information on agencies using conventional or other shared trunked systems. We could not reconcile the data provided by DOLA with the information provided by DPA and the CCNC, in part because of the lack of a standard definition of public safety and first responder agencies and differences in the types of agencies included in the data. As a result, the data could not be used to fully identify the State's inventory of public safety and first responder agencies or the types of communications systems used by these agencies.

In another attempt to determine the types of communications systems public safety agencies are using, we asked DOLA to collect information on the number of dispatch centers in the State and the types of communication systems used by the dispatch centers. As discussed previously, dispatch centers coordinate the day-to-day radio communications for public safety agencies, and a single dispatch center often serves multiple public safety disciplines, sometimes within multiple jurisdictions. According to information provided by DOLA, of the approximately 100 dispatch centers in the State, about 35 use conventional radio systems, about 30 use the statewide DTR System, about 15 use other types of shared trunked radio systems, and about 20 use both conventional and shared trunked systems. Of the about 30 dispatch centers that use the statewide DTR System, all but one are located in counties that have widespread DTR System coverage. Conversely, of the approximately 35 dispatch centers that use conventional systems, 5 are in counties where DTR System coverage is sparse. While these data suggest that the State is not yet fully interoperable, because of the lack of information on the inventory of public safety agencies in each dispatch area and the types of communications systems the agencies use, the data are insufficient to determine the additional steps needed to achieve statewide interoperability.

Communications Needs

Finally, in addition to reviewing the limited data available on statewide communications capabilities, we attempted to identify the communications needs that must be addressed for the State to attain a desired level of interoperable communications. Identifying needs and quantifying the resources required to meet those needs is the next step once communications capabilities and gaps are

identified. As discussed previously, the U.S. Department of Homeland Security requires states to identify and prioritize needs. Additionally, the statewide interoperable communications plan, due by the end of Calendar Year 2007 as a condition of receiving federal grant funds, requires DOLA to include provisions for funding or identify funding sources that can be used to improve and sustain interoperable communications.

We reviewed the extent to which DOLA has identified statewide communications needs and found that data are insufficient to comprehensively determine the additional capabilities and resources required to achieve statewide interoperability for local jurisdictions. For example, at the time of our audit, DOLA did not have comprehensive information on the number of digital trunked radios or linking devices needed by local public safety and first responder agencies to become interoperable or on the additional trainings and exercises needed for first responders to ensure agencies can establish interoperable communications during an emergency. Neither the communications capabilities self-assessments prepared by the regions nor the 2006 regional interoperable communications plans identified or quantified the needs and resources that would be required to attain interoperability. The regions provided some information on their interoperable communications needs in their 2004 through 2006 Homeland Security Grant applications. However, the individual communications projects identified by the regions in their grant requests were not part of a regional or statewide interoperable communications plan, and thus, there is no way to determine if by funding these specific projects, regions would be able to achieve full interoperability. For example, the regions requested about $23 million for interoperable communications equipment in their 2007 Homeland Security Grant requests. Without viewing these requests within the context of a regional or statewide plan, it is unclear how much unmet need will be addressed by these funds. At the state level, DPA has assessed its needs and estimates that to finish transitioning state agencies to the DTR System, it needs an additional $13 million to upgrade DTR System equipment and purchase additional radios for state agencies. DPA estimates the total cost to the State of implementing the DTR System will be approximately $68 million, which includes the estimated $13 million.

The lack of comprehensive data on statewide communications capabilities and needs prevents DOLA from being able to measure the State's progress in achieving statewide interoperable communications or identify additional needs and resources required to ensure communications preparedness during an emergency. The lack of data also hinders the State's ability to develop a viable statewide interoperable communications plan, as required by the General Assembly under the statute (Section 24-32-2116, C.R.S.) and by the U.S. Department of Homeland Security through grant requirements. To ensure sound interoperable communications planning and accountability for targeting funds, DOLA needs to implement mechanisms to collect reliable and sufficient data on current statewide

communications capabilities and needs, as well as the resources required, to achieve statewide interoperability. DOLA should also consider working with DPA, as necessary, when developing these mechanisms and collecting data to help ensure that DOLA obtains the appropriate information. DPA, as the manager of the state-owned portion of the DTR System, has technical expertise related to communications technology and could provide valuable assistance to DOLA.

Recommendation No. 1:

The Department of Local Affairs should improve the quality of statewide interoperable communications planning and ensure accountability for targeting funds by working with the Department of Personnel & Administration, as necessary, to implement mechanisms to collect reliable and sufficient data on the State's current communications capabilities and needs, as well as the resources required to achieve statewide interoperability.

Department of Local Affairs Response:

Agree. Implementation Date: June 2008.

The first portion of the recommendation regarding implementation of improvements in the quality of planning and accountability for targeting funds by working with the Department of Personnel & Administration (DPA) will be implemented by the end of December 2007, utilizing federal grant funds recently made available.

The second portion of the recommendation regarding the implementation of mechanisms for gathering reliable and sufficient data on current communications capabilities, needs, and resources required will be fully implemented in concert with DPA, the Department of Public Safety, Homeland Security Regions, and local governments by June 2008. The specific dates and extent of the data will depend in part upon resources available to effect such implementation from state, federal, and other sources.

Targeting Funds

As early as 2003, the federal government, through the Homeland Security Grant Program, emphasized the importance of allocating limited funds on the basis of risk and prioritized needs, since no state can prepare for every possible terrorist attack, disaster, or major emergency. More recently, the December 2005 National

Preparedness Goal issued by the U.S. Department of Homeland Security indicated that states must prioritize their needs, including those related to interoperable communications, and develop a strategic plan for improving preparedness based on risk and need. Similarly, the 2006 State Homeland Security Strategy prepared by DOLA and DPS states that Colorado should direct resources toward the areas with the greatest need and threat. To ensure funds are targeted to the State's most significant interoperable communications needs, data on security risks and communications needs, along with other factors, such as capabilities and available resources, must be viewed together so that funding priorities can be identified.

In Colorado, two state agencies have responsibilities that impact the State's ability to target its interoperable communications resources toward areas with the greatest risk and need. First, DOLA is responsible for distributing state and federal grant funds to state agencies and local jurisdictions for the purpose of improving statewide interoperability. During 2004 through 2006, DOLA awarded more than $44 million in Homeland Security Grants to state agencies and to local governments for the purpose of purchasing interoperable communications equipment. Federal requirements for these grants specifically directed DOLA to consider statewide risks and prioritized needs as primary factors when distributing these funds. Additionally, DOLA distributed about $35 million in Colorado Wireless Interoperability Network (CWIN) Initiative funds through Energy and Mineral Impact Grants to local governments during 2005 and 2006 to expand the statewide DTR System infrastructure.

Second, DPS is responsible for assessing statewide risks and vulnerabilities and identifying the State's critical infrastructures. Critical infrastructures are assets that if damaged or destroyed could have devastating consequences to the State with respect to its economy, public safety, and public health. Examples of critical infrastructures include reservoirs, dams, hospitals, and major highways. Information on the State's risks, vulnerabilities, and critical infrastructures is necessary for DPS to ensure the State's readiness to respond to, including communicating during, an emergency. When assessing risks and vulnerabilities, DPS considers factors such as the commerce, public health, and transportation risks in a particular area and the likelihood that a particular threat will occur. When making its assessment, DPS collects information from each of the nine all-hazards regions on the risks, vulnerabilities, and critical infrastructures in the region. DPS is responsible for compiling this information and determining which areas or critical infrastructures in the State are considered to be higher risk and most vulnerable. DPS then assigns a risk level to the region of "High," "Medium," or "Low" based on this assessment.

We reviewed DOLA's distribution of grant funds to the regions from 2004 through 2006 and found that DOLA did not sufficiently consider risk, capabilities, needs, available resources, and other relevant factors when prioritizing and allocating funds.

First, we found DOLA did not prioritize statewide interoperable communications needs on the basis of risk when making these grant distributions. We compared DPS's risk data and DOLA's Homeland Security Grant funding allocations for each of the nine regions and found problems with the correlation between risk levels and funding allocations. Although the region with the highest risk level received the most grant funds (more than $20 million), the four regions assessed at a "Medium" risk level received, in total, $9.2 million in grant funds, while the four regions assessed at a "Low" risk level received, in total, $11.1 million. One low-risk region alone received $4.5 million, which was the second highest amount of grant funds distributed for interoperable communications equipment during this period.

Second, we found that DOLA did not have a systematic method for evaluating specific funding requests for interoperable communications projects against statewide interoperable communications risk, needs, and priorities. From a statewide perspective, communications priorities from one region may not have the same weight as priorities from another region. DOLA's fragmented approach to prioritizing needs does not maximize limited funds. All state-directed funding, including Homeland Security Grants and CWIN grants allocated to improve interoperability, should be prioritized on the basis of risks and need. The importance of developing a statewide approach for prioritizing risks and needs was discussed in our October 2005 *Homeland Security Grant Program Performance Audit*.

To date about $135 million in state-directed funds has been allocated for statewide interoperability, and the State has limited additional dollars available to allocate toward improving statewide interoperable communications. It is important that these funds be directed toward improving communications capabilities in those areas with the greatest needs and highest risks. Therefore, DOLA should improve its practices for evaluating communications capabilities, needs, risks, and available resources and ensure these evaluations consider risks and priorities from a statewide perspective. Funds intended to promote interoperability from any funding source should be targeted based on statewide priorities and result in measurable improvements to statewide interoperability. DOLA should also consider working with DPS, as necessary, when evaluating statewide risks since DPS has specialized expertise in assessing public safety risks. According to DOLA, staff considered regional risk levels when making 2007 Homeland Security Grant allocations. Considering risk is a positive change in DOLA's grant allocation process and should be expanded to address statewide priorities based on the analysis of solid risk, needs, and other relevant data.

Recommendation No. 2:

The Department of Local Affairs should improve its practices for evaluating communications capabilities, needs, and risks and ensure these evaluations consider risks and priorities from a statewide perspective, working with the Department of Public Safety as necessary. Grant funds from available funding sources should be targeted toward those communications projects that address the State's greatest risks, needs, and any other relevant factors and result in measurable improvements to statewide interoperability.

Department of Local Affairs Response:

Agree. Implementation Date: June 2008.

This recommendation was adopted and implemented as a part of the State's review and recommendations on the Federal Fiscal Year 2007 grant cycle and has been institutionalized in the Homeland Security Grant review solicitation, review, and approval process for Federal Fiscal Year 2008 and future years. Other grant funds that might be made available to meet the need for communications will target projects that address the State's greatest risks, needs, and other relevant factors.

Statewide Strategic Approach

For the State to be successful in achieving statewide interoperability, it must take a strategic approach to communications planning, which includes developing an oversight mechanism for effectively implementing and enforcing its plan. Both the State Homeland Security Strategy and the National Preparedness Goal recognize the importance of interoperable communications planning. One of the goals in the State Strategy is to maintain and enhance a statewide operational plan for interoperable communications. Additionally, according to the U.S. Department of Homeland Security, statewide interoperable communications planning is important because it establishes short- and long-term strategic goals, creates a unified vision or approach, and guides the improvement of interoperable communications. Finally, state statute requires DOLA to prepare a statewide interoperable communications plan.

We reviewed the statewide approach to achieving interoperability and found that the State has not taken a coordinated and strategic approach to communications planning. As discussed in this chapter, DOLA lacks the data necessary to sufficiently assess current statewide communications capabilities and identify and

prioritize statewide communications needs. Additionally, DOLA has not targeted funds to those areas of the State with the greatest communications needs and the highest risks. Effective communications planning requires a comprehensive understanding of statewide communications capabilities, risks, and needs at both state and local levels so that funds can be targeted toward priorities that measurably further the State's goal of achieving statewide interoperability.

In contrast, the development of the state-owned portion of the DTR system, as planned and implemented by DPA, illustrates how a comprehensive, well-thought-out plan can lead to successful implementation. To prepare the DTR implementation plan, DPA worked with local governments and other stakeholders over several years to (1) obtain comprehensive information on statewide needs, (2) identify the type of system that would best meet those needs, and (3) determine the resources required to implement the system. DPA's planning process resulted in the successful implementation of a public safety radio infrastructure that has helped advance the State's efforts to achieve statewide interoperability.

In addition to comprehensive communications planning, the State must evaluate its process for overseeing and implementing the plan. According to the U.S. Department of Homeland Security, a statewide strategic approach to implementing interoperable communications is best achieved when a formal, centralized governance structure exists to guide and oversee the process. A statewide strategic approach requires continuous inter-disciplinary and inter-jurisdictional planning that considers and evaluates regional interoperability needs and priorities in the context of overall statewide preparedness.

The statutes provide limited direction on interoperable communications planning, oversight, and implementation responsibilities. Currently the State has no centralized governing structure for coordinating and overseeing interoperable communications and for developing a statewide strategic approach for planning, implementing, and funding interoperable communications. Instead, the statutes have assigned responsibilities related to interoperable communications to several different state agencies with specific expertise in particular areas. For example, DPA and the Governor's Office of Information Technology (OIT), as the state entity specifically charged by the statutes to oversee statewide technology projects, are responsible for implementing and maintaining the DTR System because of their technology expertise. DPS is responsible for assessing the State's risks, vulnerabilities, and critical infrastructures, including the State's ability to communicate during emergencies, because of DPS's expertise in collecting and assessing public safety risk information. DOLA is responsible for coordinating with local jurisdictions to distribute funds for strengthening interoperable communications because DOLA oversees Homeland Security Grants and emergency management for the State and has built relationships with the local jurisdictions for that purpose. Finally, local

jurisdictions play an important role in achieving statewide interoperability because they are typically the first to respond to emergencies. Thus, local jurisdictions are best positioned to quantify their own capabilities and needs and communicate these data to the State for planning purposes.

Although each of these departments and the local jurisdictions have specific knowledge and expertise, coordination is critical to ensure these agencies can both meet their individual responsibilities and help the State address security risks while furthering its goal of attaining statewide interoperability. A governing body that includes representatives and key personnel from public safety and first responder groups—such as law enforcement, fire safety, and emergency medical services—and from state, local, and, as appropriate, the federal government can also improve the statewide interoperable communications planning process by promoting collaboration and cooperation among stakeholders. Therefore, OIT, as the state agency responsible for overseeing statewide technology projects, should work with the General Assembly, as needed, to create a governing body for coordinating statewide interoperable communications and assigning responsibilities to this body, such as developing and maintaining the statewide interoperable communications plan as discussed below. One option may be to establish a governing body within state government, such as a state board or commission with inter-jurisdictional representation and possibly rule-making authority. Wyoming has established a commission to oversee its statewide interoperable communications planning and Utah has established a state committee for similar purposes. Another option may be to work with the General Assembly to establish a quasi-governmental agency, such as an authority that is independent from state government, to oversee statewide interoperable communications. The General Assembly would need to statutorily define the authority's governing board and membership, as well as the authority's role and responsibilities.

As part of this process, consideration will need to be given to whether the Consolidated Communications Network of Colorado (CCNC), which provides policy and operational oversight of the statewide DTR System as discussed in Chapter 2, should (1) be formalized as part of the governance structure, (2) serve in an advisory capacity to the governing body, or (3) be linked through a memorandum of understanding or intergovernmental agreement to the governing body so that both the strategic planning and oversight for interoperable communications and the operational management of the statewide DTR System are integrated. The role of the CCNC is discussed in more detail in Chapter 2, Recommendation No. 4.

Additionally, the State needs to reevaluate how to best use limited funds to improve statewide interoperable communications. According to DOLA, Colorado was recently awarded about $14 million in federal Public Safety Interoperable Communications Grant funds, a one-time federal initiative. DOLA also recently

awarded about $5.6 million in 2007 Homeland Security Grants to state agencies and local governments specifically to improve interoperable communications. To ensure all state funds are used effectively, the governing body discussed above should work with DOLA, DPA, and DPS to establish a statewide strategic approach for planning and implementing statewide interoperable communications and for targeting dollars most effectively to strengthen interoperable communications capabilities. As part of this process, the governing body should maintain and update the statewide interoperable communications plan on an ongoing basis and ensure that the plan includes a tactical component, as required by the statute (Section 24-32-2116(2), C.R.S.). The tactical component should address how first responders across the State will use their radio equipment to establish communications with responders from other disciplines and jurisdictions when an emergency occurs. The statewide plan should also sufficiently address the need for training, testing, and exercising on interoperable communications. Finally, the governing body should work with DOLA to ensure that reliable, sufficient data on statewide communications capabilities and needs are available to prepare the plan, as discussed in Recommendation No. 1. All of these steps are essential to ensuring the State is adequately prepared to respond to emergencies and to protect state residents and resources in the event of a significant disaster.

Recommendation No. 3:

The Governor's Office of Information Technology should work with the General Assembly, as needed, to evaluate options for establishing a governing body that is responsible for coordinating statewide interoperable communications, including preparing, implementing, and enforcing the statewide interoperable communications plan. The governing body that is established should work with the Office of Information Technology and the Departments of Local Affairs, Personnel & Administration, and Public Safety to establish a strategic approach for planning and implementing statewide interoperable communications and for targeting funds to strengthen interoperable communications capabilities. As part of this process, the governing body should maintain and update the statewide interoperable communications plan on an ongoing basis and ensure that it is based on reliable, sufficient data; addresses tactical operations; and includes practices for training, testing, and exercising on interoperable communications.

Governor's Office of Information Technology Response:

Agree. Implementation Date: July 2008.

The Governor's Office of Information Technology (OIT) will work with the General Assembly, when needed, to evaluate options for forming a governing body that will assist with maintaining and overseeing a statewide communications interoperability plan. OIT supports the establishment of a Statewide Interoperability Executive Committee as described in the current draft of the Statewide Communications Interoperability Plan.

Department of Local Affairs Response:

Agree. Implementation Date: June 2008.

The Department of Local Affairs will cooperate with the Governor's Office of Information Technology, the General Assembly, and the Departments of Personnel & Administration and Public Safety in evaluating the need for, and in facilitating any changes required to establish, formalize, and/or enhance, such a representative governing body and in working with such body in planning efforts.

Department of Personnel & Administration Response:

Agree. Implementation Date: June 2008.

A draft statewide communications plan has already been developed as per the requirements of Senate Bill 06-237 and through guidelines from the U.S. Department of Homeland Security and the National Telecommunications & Information Administration (NTIA) for the Public Safety Interoperable Communications Grant applications. The draft Statewide Communications Interoperability Plan (SCIP) has identified the need to establish a Statewide Interoperabilty Executive Committee (SIEC) and has created draft membership and bylaws. The draft SCIP recommends establishing the SIEC first through Executive Order and then to determine if legislation is required. The target date for the executive order is no later than December 31, 2007.

Department of Public Safety Response:

Agree. Implementation Date: July 2008.

The Colorado Department of Public Safety supports the formation and implementation of a governing body to provide an over-arching strategic approach to coordinating, implementing, and enforcing the statewide interoperability plan. To this end, a Statewide Interoperable Executive Committee (SIEC) has been proposed and suggested members identified. It appears that this Committee would fulfill the spirit of this recommendation. It has been recommended that this Committee be authorized via Executive Order and then seek legislative action if necessary. A statewide interoperable communications strategy has been recently completed pursuant to Senate Bill 06-237 and to meet the requirements of the Public Safety Interoperability Communications Grant.

This page intentionally left blank.

Digital Trunked Radio System

Chapter 2

Background

The Department of Personnel & Administration (DPA) oversees the state-owned portion of the Digital Trunked Radio (DTR) System which was originally developed to improve interoperable communications capabilities for state agencies. DPA initiated planning for the DTR System in 1991 and established a seven-phase implementation plan for transitioning state government from its multiple conventional radio systems to the DTR System beginning in Fiscal Year 1999. This plan included purchasing the radio equipment needed by state agencies and building an infrastructure of zone controllers and radio towers.

The following table shows DPA's seven-phase implementation schedule for the DTR System, the projected completion date for each phase, and the actual year of completion. As the table shows, Phases I through IV and Phase VII have been implemented. This means that if state agencies have the proper radios, they can access and use the DTR System in the counties listed in these phases. Although DPA originally estimated that Phases V and VI would be implemented by Fiscal Year 2002, these phases have not yet been completed due to funding limitations. According to DPA, Phases V and VI will be completed by the end of Calendar Year 2008 by local governments using Colorado Wireless Interoperability Network (CWIN) Initiative funds.

Department of Personnel & Administration
Digital Trunked Radio (DTR) System[1]
Implementation Phases and Status
As of September 2007

Project Phase	Counties	Projected Fiscal Year of Completion	Actual Fiscal Year Completed
I	Arapahoe, Denver, Douglas, Jefferson	1999	2000
II	Adams, Broomfield, Boulder, Clear Creek, Gilpin	2000	2000
III	Elbert, Weld, Morgan, Larimer, Phillips, Sedgwick, Yuma, Washington, Kit Carson, Cheyenne, Lincoln, Logan	2001	2001
IV	El Paso, Pueblo, Fremont, Teller, Custer, Otero, Las Animas, Huerfano, Baca, Prowers, Bent, Kiowa, Crowley, Park, Chaffee	2002	2002
V	Mesa, Garfield, Rio Blanco, Routt, Moffat, Grand, Jackson, Pitkin, Lake, Eagle, Summit	2002	In Progress[2]
VI	Archuleta, San Juan, Hinsdale, Montrose, Gunnison, Ouray, La Plata, San Miguel, Dolores, Montezuma, Delta	2002	In Progress[2]
VII	Costilla, Conejos, Saguache, Alamosa, Rio Grande, Mineral	2004	2005

Source: Department of Personnel & Administration.

[1] This table only includes information on the implementation status of the state-owned portion of the DTR System. Local governments have also contributed to the build-out of the statewide DTR System. This table does not reflect DTR System build-out completed by local governments.

[2] Phases V and VI are being completed by local governments through the Department of Local Affair's Colorado Wireless Interoperability Network (CWIN) Initiative funded by the State's Energy and Mineral Impact Grants. DPA estimates that these phases will be complete by the end of Calendar Year 2008.

The General Assembly created the Public Safety Communications Trust Fund (the Fund) in 1998 to record and track activity related to the acquisition and maintenance of the DTR System for state government. Pursuant to the statute (Section 24-30-903(1)(i), C.R.S.), DPA is responsible for administering the Fund. This includes acquiring and maintaining the necessary system equipment for the State's operations—such as radios and radio accessories—and infrastructure—such as transmitter or radio towers. DPA is also responsible for maintaining financial records for the Fund on the State's financial system that are accurate and complete.

DPA has received almost $57 million to build the infrastructure for the state-owned portion of the DTR System and to purchase radios for state agencies. Of this total, the General Assembly appropriated about $47.5 million in state capital construction funds to the Fund during Fiscal Years 1999 through 2001 for implementing the DTR System. Overall, the Fund has received about $3.4 million in interest income. Additionally, as discussed in the Description Chapter, DPA has received about $5.7 million in federal grant funds to help further implementation of the DTR System. Federal funds are recorded in the State's General Fund, as opposed to the Public Safety Communications Trust Fund.

DPA estimates that it needs about $13 million in additional funding to upgrade the state-owned portion of the DTR System and to purchase additional radios for state agencies. If DPA receives this additional funding, the state-owned portion of the DTR System will cost a total of about $68 million, or about $11 million less than the $79 million originally estimated for the project. The following table shows DPA's revenue and expenditures for the state-owned portion of the DTR System for Fiscal Years 1999 through 2007.

Department of Personnel & Administration
Funding for the State-Owned Portion of the Digital Trunked Radio (DTR) System
Revenue and Expenditures
Fiscal Years 1999 through 2007

	FY 1999	FY 2000	FY 2001	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007	Total
Revenue										
Capital Construction	$3,300,000	$27,555,000	$16,655,000	$0	$0	$0	$0	$0	$0	$47,510,000
Interest Income	$178,000	$129,000	$1,193,000	$1,116,000	$355,000	$121,000	$128,000	$115,000	$109,000	$3,444,000
Federal Grants[1]	$0	$0	$0	$0	$0	$2,451,000	$2,105,000	$934,000	$247,000	$5,737,000
Total Revenue	**$3,478,000**	**$27,684,000**	**$17,848,000**	**$1,116,000**	**$355,000**	**$2,572,000**	**$2,233,000**	**$1,049,000**	**$356,000**	**$56,691,000**
Expenditures										
Property[2]	$0	$10,204,000	$5,337,000	$21,413,000	$4,823,000	$3,465,000	$1,992,000	$915,000	$247,000	$48,396,000
Personal Services	$0	$0	$0	$57,000	$2,000	$0	$79,000	$0	$0	$138,000
Operating	$0	$42,000	$2,202,000	$455,000	$318,000	$184,000	$923,000	$18,000	$0	$4,142,000
Travel	$0	$8,000	$3,000	$9,000	$1,000	$1,000	$0	$0	$0	$22,000
Transfers	$0	$0	$0	$0	$445,000	$0	$217,000	$425,000	$650,000	$1,737,000
Total Expenditures	**$0**	**$10,254,000**	**$7,542,000**	**$21,934,000**	**$5,589,000**	**$3,650,000**	**$3,211,000**	**$1,358,000**	**$897,000**	**$54,435,000**

Source: Colorado Financial Reporting System. Revenue and expenditures related to the Digital Trunked Radio (DTR) System are recorded in either the Public Safety Communications Trust Fund or the General Fund, depending on the funding source.

[1] Federal grants revenue includes about $4,116,000 from the Homeland Security Grant Program, $994,000 from the Community Oriented Policing Services (COPS) 2003 Technology Grant, $543,000 from the U.S. Office of Justice Programs, and $84,000 from the Chemical Stockpile Emergency Preparedness Program. Federal grants are recorded in the General Fund.

[2] Property includes items such as equipment and infrastructure.

In addition to administering the Fund, DPA is required by the statute (Section 24-30-903(1)(e), C.R.S.) to "establish telecommunications procedures, standards, and records for management of telecommunications networks and facilities for all state departments, institutions, and agencies." DPA works with the Consolidated Communications Network of Colorado (CCNC) to carry out this statutory mandate. As discussed previously, the CCNC is a public nonprofit corporation that is a users group that exists to "assist in the development of facilities, operational procedures, maintenance, grants, and training for the statewide digital trunking radio network." The State and all local and federal agencies that use the DTR System are members of the CCNC. The CCNC is governed by a 36-member Board of Directors elected by user agencies and an 11-member Executive Directors Committee elected by the Board of Directors.

The statute (Section 24-30-908.5(6), C.R.S.) authorizes the State Auditor to investigate the affairs of the Fund and requires the Legislative Audit Committee to review the expenditures from the Fund every two years. Our audit reviewed DPA's management of the DTR System and the Fund. Specifically, we reviewed DPA's participation in the CCNC, disaster recovery planning for the DTR System, and the training of state engineers and technicians responsible for maintaining the DTR System. In addition, we reviewed the financial records of the Fund, including DPA's capitalization and depreciation of the DTR System and inventory controls for digital trunked radios. We also reviewed DPA's controls over disbursements from the Fund for the period of May 1, 2005, through June 30, 2007. We identified areas for improvement, as discussed throughout this chapter.

CCNC Participation

As discussed previously, the Consolidated Communications Network of Colorado (CCNC) is a public nonprofit corporation. The CCNC has about 700 state agency and local government members—500 of which use the statewide DTR System as their primary communications system and 200 of which use the statewide DTR System as their secondary or tertiary communications system. The CCNC was created by an employee of a participating local government in 2002 to address operational issues and to facilitate cooperation among state, local, and federal government agencies that share ownership and/or use of the statewide DTR System. As of September 2007, the statewide DTR System was composed of three zone controllers and 144 radio towers. The State owns two of the zone controllers and 78 (54 percent) of the radio towers. Local governments own the third zone controller and the remaining 66 (46 percent) radio towers. The CCNC, through its Board of Directors and Executive Directors Committee, has established membership requirements, standard operating procedures, and a service level agreement for using and maintaining the statewide DTR System. The Director of Telecommunications

for the State, a position within DPA, is a permanent member of the CCNC Executive Directors Committee.

Title 29, Article 1, Part 2 of the Colorado Revised Statutes sets forth the requirements for establishing intergovernmental relationships, such as the CCNC. We reviewed the statutes and determined that it is unclear whether DPA has authority to participate in the CCNC under current law. According to the statute:

> Governments may cooperate or contract with one another to provide any function, service, or facility lawfully authorized to each of the cooperating or contracting units . . . only if such cooperation or contracts are authorized by each party thereto **with the approval of its legislative body or other authority having the power to so approve** [emphasis added]**.** (Section 29-1-203(1), C.R.S.)

The CCNC is composed of multiple governmental agencies cooperating with one another to manage the statewide DTR System and thus, according to the statute, DPA's participation in the CCNC must be approved by the General Assembly. The General Assembly has recognized the importance of having the State and local governments work together with respect to the DTR System to help achieve statewide interoperable communications. In Section 24-30-903, C.R.S., the General Assembly directed DPA to work with local, state, and federal agencies to develop a long-range telecommunications plan for state agencies that addresses public safety radio communications systems. Additionally, this statute directs DPA to carry out its duties and responsibilities associated with the DTR System in a manner that is consistent with the objective of maximizing access to the System for all levels of government. In response to this statutory mandate, agencies at the local, state, and federal level participated with DPA in planning and implementing the statewide DTR System. Although the statutes indicate that it is the General Assembly's intent that DPA work with local and federal agencies with respect to the statewide DTR System, it is not clear that this intent constitutes specific approval for DPA to participate in the CCNC as required by the laws governing intergovernmental relationships set forth in Section 29-1-203, C.R.S.

Participation in the CCNC, without the explicit approval of the General Assembly, may present risks to the State. In effect, DPA has informally delegated some of its responsibilities related to managing the state-owned components of the DTR System to the CCNC without retaining sufficient decision-making authority over these components. For example, as previously discussed, the CCNC has established standard operating procedures for the System and a service level agreement that includes a response plan for system outages and minimum training requirements for staff at each participating agency who are responsible for maintaining the System (as discussed in Recommendation No. 6). This means that DPA has ceded to a

nongovernmental entity—the CCNC—the authority to determine how state-owned infrastructure and equipment will be used and maintained without the General Assembly approving such delegation of authority.

Additionally, as the statewide DTR System continues to expand, effective management of the System is increasingly critical to ensuring first responders and public safety agencies are able to communicate during emergencies. However, as discussed later in this chapter, neither the State nor the CCNC has updated the disaster recovery plan for the statewide DTR System, a key protection that would ensure the System could be recovered if disabled during an emergency or disaster. Furthermore, DPA and local agencies report that, since the CCNC is a volunteer organization, certain important functions are not always handled timely. For example, DPA and local agencies report there are backlogs in the CCNC's assignment of talk groups to user agencies. Even though an agency may be in a DTR System coverage area and have radios that operate on the statewide DTR System, the agency cannot use the System until the agency is assigned to a talk group that can access the statewide DTR System.

Finally, since the CCNC is a nongovernmental entity and was created outside of the legislative process, there has been no formal opportunity for public input into this arrangement. Although DPA retains a seat on the Executive Directors Committee, which is responsible for the daily administration, operation, and financial affairs of the CCNC, DPA represents only 1 vote out of 11. Therefore, while the State presently owns the majority of the statewide DTR System, it is possible that the CCNC could make decisions regarding the System that are not in the State's best interest. Furthermore, as more local government agencies purchase equipment and participate in the DTR System, the State may own a smaller proportion of the statewide DTR System. Thus, the State may have less of a voice in the management of the System, even as the importance of the statewide DTR System to emergency response statewide increases.

As discussed in Chapter 1, achieving statewide interoperable communications is a primary state and national homeland security goal, and the foundation underlying interoperable communications is the ability of public safety and first responder agencies across jurisdictions (e.g., state and local governments) to communicate with one another. The General Assembly has recognized the importance of having the State and local governments work together with respect to the DTR System to help achieve statewide interoperable communications. Clearly, there is a need for cooperation among all DTR System users, including the State and local and federal agencies, to oversee and manage the statewide DTR System through a mechanism such as the CCNC.

Since DPA's authority to participate in the CCNC is unclear and effective management of the statewide DTR System is of critical importance, it may be an appropriate time for DPA to work with local governments to reevaluate the role of the CCNC. As part of this evaluation process, DPA should seek a legal opinion from the Attorney General's Office regarding DPA's authority to participate in the CCNC. Additionally, DPA should determine if the CCNC is the best mechanism for managing the statewide DTR System, a key component to the State's effort to attain interoperability. DPA should evaluate alternatives that allow the Department to fulfill its responsibilities to the State with respect to the System and also allow for collaboration with and participation from local governments.

Depending on the opinion prepared by the Attorney General, one alternative may be for DPA to seek specific statutory authority to participate in the CCNC. This would provide an opportunity for public input into the decision and allow the General Assembly to decide whether this arrangement is in the State's best interests. This approach would require clarifying the role and responsibilities of the CCNC and defining any financial implications related to the State's participation. Other alternatives may include (1) incorporating the current functions of the CCNC as part of, or advisory to, the governing structure discussed in Chapter 1 or (2) formalizing the CCNC's relationship with the governing structure through a memorandum of understanding or intergovernmental agreement. Regardless of the alternative selected, DPA will need to work with local governments to establish a linkage between the CCNC and the governing structure for statewide interoperable communications to ensure the responsibilities of each are clear.

Recommendation No. 4:

The Department of Personnel & Administration should improve the oversight and management of the statewide Digital Trunked Radio System by:

a. Seeking a legal opinion from the Attorney General's Office to determine whether the Department is statutorily authorized to participate in the Consolidated Communications Network of Colorado (CCNC).

b. Working with local governments to evaluate alternatives for managing the statewide Digital Trunked Radio System that will further the State's goal of achieving statewide interoperability while protecting the State's interests. Depending on the outcome of the Attorney General's opinion, alternatives could include seeking specific statutory authority to participate in the CCNC, formalizing the functions of the CCNC as part of, or advisory to, the governance structure discussed in Recommendation No. 3, or formalizing the relationship between the CCNC and the governing structure for statewide

interoperable communications through a memorandum of understanding or intergovernmental agreement.

Department of Personnel & Administration Response:

Agree. Implementation Date: June 2008.

a. The Department of Personnel & Administration agrees to seek a legal opinion from the Attorney General's Office regarding whether the Department is statutorily authorized to participate in the CCNC.

b. This is a continuing and ongoing effort of the Department. Currently the Department of Personnel & Administration works with the local governments on a monthly basis via the CCNC Technical and Operations Committee to evaluate alternatives for managing the DTR System. The Department will evaluate options for formalizing the relationship between the CCNC and the Department through a memorandum of understanding or intergovernmental agreement. The relationship between the Department and the CCNC is a major factor in the success of the DTR System project and its capabilities. The CCNC has established unprecedented collaboration and cooperation between the State and local, tribal, and federal agencies.

Disaster Recovery Planning

Information system disaster recovery is essential if government is to continue providing critical services in the event of natural or man-made disruptions or disasters. Disaster recovery planning refers to the process of identifying, testing, and evaluating all of the resources and procedures needed to make specific information system-based functions of an organization operational after a disruption in service. While state agencies have long been required to have disaster recovery plans in place, in 2006 the Colorado Chief Information Security Officer (CISO) issued a disaster recovery policy that requires every state public agency, as defined in Section 24-37.5-102(5), C.R.S., to develop disaster recovery plans for information technology systems "to reduce the impact of a major disruption on key business functions and processes." According to the policy, agency disaster recovery plans are to include the following components:

- **Roles, responsibilities, and contact information** for the individuals responsible for implementing the disaster recovery plan.

- **Recovery time frames** outlining both response and recovery requirements.

- **Recovery procedures** detailing the ways in which services will be restored and operations returned to normal.

- **Plan training** on a regular basis for the individuals with roles and responsibilities in implementing the disaster recovery plan.

- **Plan testing** on a regular basis to ensure services can be effectively restored and any problems addressed.

- **Plan maintenance** to ensure the plan is updated or modified to reflect changes in recovery requirements, time frames, personnel, or other factors. The plan should also include procedures for distributing the plan to stakeholders and notifying stakeholders of any changes to the plan.

The DTR System is an information system that uses computers and microwave transmitters to network the radio transmitter towers located throughout the State and to assign frequencies, or channels, to users when needed. As with all information systems, the DTR System could be damaged or severely disrupted if a disaster or an emergency occurred. Possible disasters that could affect the DTR System include natural ones, such as lightning, fires, tornadoes, and floods, and those that are man-made, including acts of terrorism and vandalism. Therefore, a disaster recovery plan is necessary to ensure that radio service is still available to support critical state functions, such as law enforcement or emergency services, in the event of a disaster. DPA first created a disaster recovery plan for the DTR System in 2002 and last updated the plan in 2003.

We reviewed DPA's disaster recovery plan for the state-owned portion of the DTR System and identified problems in two areas. First, we found DPA may not be adequately testing its disaster recovery plan as required by the CISO disaster recovery policy. Currently DPA tests its plan during routine system upgrades. Performing system upgrades usually requires DPA to disable portions of the DTR System for a period of time. This allows DPA to test its ability to quickly notify System users of possible disruptions in service and to implement recovery procedures to resume operations. However, it does not prepare the disaster recovery team to repair System failures under the extraordinary demands and pressures of an actual disaster or emergency. This is because system upgrades involve detailed organization and preplanning, while emergency conditions require immediate unexpected response.

Second, we found that DPA needs to document all required procedures in its disaster recovery plan and maintain the plan, including updating the plan on a quarterly basis,

as required by the CISO disaster recovery policy. As discussed above, DPA's current disaster recovery plan has not been updated since 2003.

Many state and local public safety agencies rely upon the statewide DTR System as their primary communications system. Therefore, it is important that the system be available at all times, particularly when a disaster or emergency occurs. DPA has been designated by the statute (Section 24-30-903(1)(e), C.R.S.) as the agency responsible for establishing "telecommunications procedures, standards, and records for management of telecommunications networks and facilities for all state departments, institutions, and agencies." DPA has a responsibility to comply with the CISO disaster recovery policy. Therefore, DPA should ensure there is an updated, comprehensive disaster recovery plan for the state-owned portion of the DTR System that addresses all of the critical components identified in the CISO disaster recovery policy. Once a decision is made regarding the management of the statewide DTR System, as discussed in Recommendation No. 4, DPA should help develop a disaster recovery plan for the entire statewide system, including locally owned infrastructure. This would likely require working with the CCNC or any other alternative structure as set forth in the statute. Finally, DPA should ensure that staff are prepared to implement the disaster recovery plan when a disaster or an emergency occurs. This could be accomplished by conducting timed tabletop exercises in which the disaster recovery team must develop a response plan to a plausible system disaster under simulated emergency conditions.

Recommendation No. 5:

The Department of Personnel & Administration should improve disaster recovery planning and preparedness for the Digital Trunked Radio System by:

a. Ensuring there is a current and comprehensive disaster recovery plan for the state-owned portion of the System. The plan should address all of the critical components of the disaster recovery policy issued by the Colorado Chief Information Security Officer.

b. Developing and maintaining a disaster recovery plan for the entire statewide Digital Trunked Radio System, including locally owned infrastructure. The Department should work with the Consolidated Communications Network of Colorado or other structure, depending on the alternative chosen in response to Recommendation No. 4.

c. Conducting tabletop exercises under simulated emergency conditions to test and improve the disaster recovery team's preparedness for plausible system disasters.

Department of Personnel & Administration Response:

Agree. Implementation Date: June 2008.

a. The Department of Personnel & Administration agrees to update the current DTR System disaster recovery plan for the state-owned portion of the System. This updated plan will address all of the critical components outlined in the December 2006 version of the policy by the Colorado Chief Information Security Officer. It should be pointed out that the disaster recovery plan was initially drafted by Department staff and provided to the CCNC for review, additions, and adoption. Most of the out-of-compliance security issues were identified in the Chief Information Security Officers' Risk-based Gap Analysis performed in early 2007. Recommendations were to upgrade the DTR System to the new current operating platform when funding was appropriated.

b. The Department of Personnel & Administration agrees to work with the CCNC to develop and maintain a disaster recovery plan for the entire statewide DTR System depending on the outcome from the Attorney General's Office regarding whether the Department is statutorily authorized to participate in the CCNC.

c. The Department of Personnel & Administration already performs real time emergency conditions that test the DTR System through site and System upgrades, during connectivity outages, and human operator induced situations. The Department will also conduct tabletop exercises for various scenarios with the disaster recovery team. Plausible system disasters can only be rectified at the time of the failure. The DTR System was designed with multiple levels of hardware redundancy to minimize a catastrophic failure.

System Training

DPA maintains the state-owned portion of the DTR System, including zone controllers and transmitter sites, to ensure that the System operates properly and that users can communicate with one another. Zone controllers are microprocessors that control and connect, or link, the remote radio towers. Radio towers are the transmitter sites located throughout the State that assign channels, or frequencies, to users. There are two state-owned zone controllers and 78 state-owned transmitter sites, or radio towers, across the State.

In June 2006 the Consolidated Communications Network of Colorado (CCNC) established minimum training requirements for all engineers and technicians responsible for maintaining zone controllers and transmitter sites. These requirements apply to Department staff, as well as any local or contract engineers or technicians, who work on state and locally owned parts of the System. The CCNC requires that zone controller engineers complete seven specific courses offered by Motorola, the System vendor, and that transmitter site technicians complete six specific Motorola courses. These courses address the architecture and management of the DTR System's operating system.

We reviewed DPA's training records for the State's two zone controller engineers and 13 of the State's 28 transmitter site technicians to assess compliance with the CCNC's minimum training requirements. We found that none of the 15 engineers and technicians reviewed has completed all of the required courses. Specifically, we found that each of the two zone controller engineers has taken only four of the seven required courses. Additionally, we found 6 of the 13 transmitter site technicians in our sample have not taken any of the required courses, and the remaining 7 technicians have only taken one or two of the required courses.

One reason that staff are not complying with the CCNC's minimum training requirements is that the requirements have been in place for less than a year and a half. Additionally, DPA reports that it does not have the financial or staff resources necessary to send all of its engineers and technicians to the trainings. On the basis of information provided by Motorola, we estimate that it would cost about $109,000 in course fees and 195 days of staff time for these 15 employees to comply with the CCNC training requirements. This estimate does not include costs for traveling to Motorola's out-of-state training locations, or alternatively, travel costs for Motorola instructors to provide training in Colorado. Finally, according to DPA, some staff already possess the skills and knowledge required by the CCNC training policy, and therefore, it is not necessary to send these employees to the trainings.

More than $54 million has been invested in the state-owned components of the DTR System. Additionally, about half of the approximately 100 dispatch centers in the State rely on the System as a primary communications system. If the engineers and technicians working on the System do not have sufficient training, errors could occur causing a zone controller or transmitter site to go offline and disrupt critical communications for users.

DPA should work with the CCNC, or any other alternative structure established in response to Recommendation No. 4, to reevaluate the current training requirements and identify cost-effective alternatives for staff to receive the necessary training. One option would be for DPA to develop a train-the-trainer program in which several employees attend the Motorola-provided training and then use the information

obtained from this training to train their colleagues. DPA could also coordinate this approach with local governments to share training expenses. Another option would be for DPA to work with the CCNC, or any other alternative structure established in response to Recommendation No. 4, to exempt employees from training requirements on a case-by-case basis if employees can provide sufficient documentation or if their supervisors can attest to the employees' proficiency in the subject matter.

Recommendation No. 6:

The Department of Personnel & Administration should work with the Consolidated Communications Network of Colorado, or any other alternative structure established in response to Recommendation No. 4, to evaluate options to ensure that staff responsible for maintaining the Digital Trunked Radio System receive the appropriate and necessary training. This should include:

a. Reviewing the appropriateness of current minimum training requirements and making any necessary revisions.

b. Identifying alternatives for engineers and technicians to receive the necessary training and exploring ways for sharing training costs with local governments, such as a train-the-trainer program.

c. Considering exempting employees from training requirements on a case-by-case basis if employees provide sufficient documentation or if supervisors attest to the employees' proficiency in the subject matter.

Department of Personnel & Administration Response:

Agree. Implementation Date: June 2008.

a. The Department of Personnel & Administration agrees to work with the CCNC to review the appropriateness of current minimum training requirements and make necessary revisions to the DTR System service level agreement as needed. It should be pointed out that the service level agreement was initially drafted by Department staff and provided to the CCNC for review, additions, and adoption.

b. The Department of Personnel & Administration agrees to explore alternatives for personnel to receive the necessary training by sharing

training costs and incorporating train-the-trainer programs. The Department has recently announced a $1,500 personal training budget allocation per individual that, if pooled, could provide funding for the necessary training.

c. The Department of Personnel & Administration agrees to explore the possibility of exempting employees from certain training requirements on a case-by-case basis when an employee demonstrates proficiency and expertise in particular subject matters.

Public Safety Communications Trust Fund

DPA is responsible for administering the Public Safety Communications Trust Fund (the Fund), which includes authorizing distributions from the Fund. According to the statute (Section 24-30-908.5, C.R.S.), the primary purpose of distributions from the Fund is for the acquisition and maintenance of public safety communications systems for use by state agencies. The statute requires DPA to keep an accurate account of all activities related to the Fund, including its receipts and expenditures. We reviewed DPA's accounting practices for the Fund and identified issues related to DPA's capitalization of assets, inventory procedures for capital assets, and controls over disbursements. These issues are discussed in the next three sections.

Capital Assets

The Fiscal Procedures Manual (the Manual) published by the Office of the State Controller defines capital assets as "long-lived assets, owned by the State, that are held primarily for use in an agency's operations and programs." Examples of capital assets include land, buildings, equipment, and infrastructure. The Manual requires that capital assets with a useful life greater than one year be capitalized if they meet established cost thresholds. The cost thresholds vary depending on the type of capital asset. For example, equipment that costs $5,000 or more and infrastructure that costs $500,000 or more must be capitalized. According to the Manual, an agency may select a lower minimum dollar threshold to capitalize the purchase of an asset, but an agency may not choose a higher dollar threshold. Once the decision is made to capitalize an asset, the cost of that asset is depreciated over its estimated useful life, as determined by the state agency.

We reviewed DPA's capitalization of expenditures from the Fund, which tracks the acquisition and maintenance costs of the state-owned portion of the DTR System.

DPA has elected to capitalize all equipment and infrastructure purchased as part of the DTR System, regardless of cost, as allowed by the Manual. However, we found DPA cannot substantiate the basis for capitalizing repair and maintenance costs or the estimated useful life used in the capitalization of these and other Fund expenditures.

Repair and Maintenance Costs. According to the Manual, agencies can capitalize repair and maintenance costs if the maintenance or repairs increase the capacity or operating efficiency, or extend the useful life of the asset. If the maintenance or repair costs meet any one of these criteria and the agency maintains documentation showing how the repair or maintenance costs enhanced the asset or extended its useful life, the costs can be capitalized along with the asset. If an expenditure serves only to restore a capital asset to working condition and does not enhance or extend the useful life of the asset, the agency should record the expenditure as a repair and maintenance expense and not capitalize it.

We reviewed DPA's capitalization of expenditures made from the Fund between July 1, 1999, and June 30, 2007, and found that DPA capitalized about $1.3 million in repair and maintenance expenditures during this period. Of the $1.3 million, we reviewed about $573,000 in expenditures made between May 1, 2005, and June 30, 2007, and found that DPA had no documentation to show that these repair and maintenance expenditures enhanced or extended the useful life of these assets. We also found that about $1,200 of these expenditures was for radio repairs. Since these expenditures would not appear to enhance the System or extend its life, it appears these costs should not have been capitalized.

Currently DPA capitalizes all expenditures from the Fund at the end of the fiscal year. Inappropriately capitalizing routine repair and maintenance expenditures can result in overstating assets and understating expenditures in the State's financial statements. DPA should take steps to ensure that repair and maintenance costs are recorded appropriately in accordance with the Manual. This should include establishing procedures to ensure all repair and maintenance costs are analyzed and classified appropriately in accordance with the Manual. If repair and maintenance expenditures meet the criteria for capitalization, DPA should capitalize the costs and maintain sufficient documentation to support that treatment. In addition, DPA should review its accounting records from prior years and make any necessary adjustments.

Estimated Useful Life. According to the Manual, the estimated useful life of a capital asset is a function of each agency's own experience, but the agency must be able to substantiate the estimated useful life that is used when capitalizing an asset. The Manual lists engineering studies, documented actual experience, and third-party regulatory requirements as examples of adequate support for determining the

estimated useful life of an asset or group of assets. The Manual also provides guidelines on the estimated useful life of certain types of assets that agencies may use if they have no supportable estimates of their own. For example, the guidelines recommend an estimated useful life of 10 years for non-office equipment.

We reviewed DPA's capitalization of DTR System equipment (e.g., radios and radio accessories) and infrastructure (e.g., transmitter sites/radio towers) and found that DPA has no documentation to substantiate the estimated useful life used to depreciate these assets. DPA depreciates all DTR System equipment and infrastructure based on an estimated useful life of 15 years. According to DPA, this useful life was determined by Department staff based on experience in the industry. However, DPA does not have any documentation to support this determination.

We also found that state and federal estimated useful life guidelines suggest that 15 years may not be an appropriate useful life for all components of the DTR System. According to the useful life guidelines provided in the Manual, non-office equipment, which would include radio equipment, has an estimated useful life of 10 years. Additionally, federal Internal Revenue Service guidelines provide an estimated useful life of six years for radio and television broadcasting equipment. This suggests that DPA's 15-year estimated useful life may be too long for radio equipment.

Using an appropriate and reasonable estimated useful life for depreciating capital assets is important because it affects the value of the State's assets and the amount of depreciation expense recorded in the State's financial statements. Agencies also need to use reasonable estimated useful lives to adequately plan for asset replacement costs. DPA should review the appropriateness of its useful life estimates for DTR System equipment and infrastructure and ensure that the estimates used by DPA are reasonable and substantiated with supporting documentation. If DPA chooses to modify its useful life estimate, it should make adjustments to accounting records as necessary.

Recommendation No. 7:

The Department of Personnel & Administration should improve its accounting of capital assets for the Digital Trunked Radio System by:

a. Establishing procedures for ensuring all repair and maintenance costs are analyzed and classified appropriately in accordance with the Fiscal Procedures Manual. If costs are capitalized, appropriate documentation to support those costs and the justification for this treatment should be maintained.

b. Reviewing the appropriateness of the estimated 15-year useful life used for depreciating all the components of the Digital Trunked Radio System, and ensuring that the estimated useful life used by the Department for each component is reasonable and substantiated with supporting documentation.

c. Adjusting, as necessary pursuant to parts (a) and (b), the State's accounting records.

Department of Personnel & Administration Response:

Agree. Implementation Date: November 2008.

The Department will ensure all repair and maintenance costs are properly analyzed and all capitalized items are properly documented. The Department also will review and document the appropriateness of a 15-year useful life. The Department will make all necessary adjustments on the above.

Radio Inventory

The DTR System consists of a variety of equipment, such as radios and radio accessories, and infrastructure, such as radio towers, located throughout the State. The state-owned portion of the DTR System cost more than $54 million. The statute (Section 24-17-102, C.R.S.) directs state agencies to institute and maintain systems of internal accounting and administrative control that ensure the proper safeguarding of state assets. Additionally, State Fiscal Rules require state agencies to ensure that all equipment owned by the State is properly accounted for when acquired, inventoried and safeguarded throughout its useful life, and properly accounted for at the time of disposal. According to the Manual, state agencies should conduct an annual physical inventory at or near year-end of all capital assets and record any necessary adjustments in the accounting records for the fiscal year.

Our previous audits of the Public Safety Communications Trust Fund recommended that DPA improve its inventory controls over radios purchased as part of the DTR System. Specifically, our May 2004 report recommended DPA conduct an annual physical inventory of the digital trunked radios assigned to state agencies by having each agency attest to its possession of the radios. DPA began conducting an annual physical inventory of digital trunked radios in Fiscal Year 2005.

We reviewed DPA's physical inventory procedures and its Fiscal Year 2006 physical inventory of digital trunked radios. We found that DPA is conducting its annual

physical inventory of all state-owned digital trunked radios after fiscal year end and recording any necessary adjustments to capital assets in the accounting records for the *following* fiscal year. For example, DPA initiated its Fiscal Year 2006 physical inventory on July 5, 2006, the beginning of Fiscal Year 2007. The physical inventory included about 6,700 radios owned and capitalized by DPA and about 700 radios owned by other state agencies. Despite not receiving responses to the physical inventory from all state agencies assigned radios, DPA ended its Fiscal Year 2006 inventory in July 2007. During this inventory, DPA identified changes in Department-owned radios resulting in a decrease of $10,800 in capital assets. However, DPA recorded this adjustment in capital assets in its accounting records for Fiscal Year 2007. As discussed above, the Manual provides that any adjustments be made in the year that the inventory was to occur.

According to DPA, the digital trunked radio inventory and adjustment process is difficult to complete within the appropriate fiscal year because DPA must depend on the assistance and cooperation of other state agencies that have been assigned the radios. Many of the state agencies in possession of the radios either do not respond to DPA's inventory request or cannot confirm the existence of the radios assigned to them. For example, in Fiscal Year 2006, DPA records indicated that the State had about 7,400 radios assigned to state agencies. However, only 5 of the approximately 7,400 radios (less than 1 percent) were actually in DPA's possession, and the remainder had been assigned to about 120 other state agencies. We found that as of June 2007, about 60 of the 120 other agencies, which had been assigned about 2,500 of the total 7,400 radios (34 percent), did not respond to DPA's request that they confirm their digital trunked radio inventory. Additionally, the other 60 agencies that did respond to DPA's request did not confirm the existence and/or the working condition of about 350 of the 4,900 radios assigned to them. This means that DPA could not account for about 2,850, or 38 percent, of the radios without searching the electronic DTR System log for each of these radios to determine the last time each radio was used and following up with the respective agency. This is a very time-consuming and resource-intensive process.

It is important that DPA complete its physical inventory of digital trunked radios in a timely manner for several reasons. First, each agency that receives the radios is responsible for safeguarding these state assets. Conducting a physical inventory helps identify radios that have been damaged, lost, or stolen, which is a public safety and accountability concern. If a radio has been lost or stolen, DPA can deactivate the radio to prevent misuse, such as unauthorized eavesdropping on potentially confidential conversations. Second, for financial statement purposes, DPA must adjust the value of its capital assets when radios owned by DPA are no longer usable or have been lost. Finally, DPA charges each of the state agencies assigned radios a monthly communications services fee that is based on the percentage of state-owned radios assigned to the agency. This fee covers DPA's costs associated with

communications services including materials, supplies, labor, and overhead. If the physical inventory is not accurate and timely, some agencies may not be charged appropriately for the radios they actually possess.

DPA needs to improve its physical inventory processes for digital trunked radios. This should include conducting the physical inventory earlier and adjusting the value of capital assets, as necessary, before fiscal year end. DPA should also continue working with state agencies to increase cooperation with and the timeliness of the physical inventory process. If DPA cannot complete its physical inventory within the time frame established by the Manual, DPA should work with the Office of the State Controller to identify an acceptable solution. In addition, when DPA upgrades the software for the DTR System, it should consider system upgrades that would allow DPA to electronically identify radios that have not been used within a certain time frame. DPA could then more easily follow up with the agencies assigned the radios to determine if they have been damaged, destroyed, lost, or stolen. According to Department staff, these types of upgrades are available.

Recommendation No. 8:

The Department of Personnel & Administration should improve its physical inventory of radios for the Digital Trunked Radio System by:

a. Conducting the physical inventory and adjusting capital assets before fiscal year end in accordance with the Fiscal Procedures Manual.

b. Continuing to work with state agencies to improve their cooperation with the Department's physical inventory process.

c. Considering upgrades to the Digital Trunked Radio System's reporting capabilities so that the System can be used to electronically identify radios that may be damaged, destroyed, lost, or stolen.

Department of Personnel & Administration Response:

Agree. Implementation Date: July 2008.

In order to ensure inventory adjustments are received in time to make year-end adjustments, the Department will conduct a physical inventory as of March. Starting the process sooner should allow staff to receive agency

responses, verify changes, check inaccuracies, and make adjustments in COFRS by the close of the fiscal year.

The Department will consider DTR System reporting system upgrades; however, any upgrades will require additional funding from the General Assembly.

Controls Over Disbursements

State Fiscal Rules require state agencies to implement internal accounting and administrative controls that reasonably ensure financial transactions are accurate and reliable, and conform to State Fiscal Rules. This includes designing and implementing programs and controls to prevent, deter, and detect fraud. Controls over disbursements are one type of internal control that can be implemented to ensure payments made to vendors are legitimate and for approved purposes.

The Fund is used by DPA to pay for the equipment, infrastructure, and maintenance associated with the DTR System. When a purchase is necessary, the Division of Information Technologies (Division) within DPA makes the purchase and gives initial approval of the vendor invoice for payment once the goods or services have been received. After the Division approves the invoice for payment, DPA's finance office is responsible for reviewing the invoice and any supporting documentation, such as a receiving slip, to verify that goods or services were received before approving the payment to the vendor.

We reviewed DPA's payment controls over disbursements from the Fund and found that improvements can be made. Specifically, we reviewed 19 payment vouchers that accounted for about $640,000 of the $1.9 million in total expenditures made from the Fund between May 1, 2005, and June 30, 2007. We identified three payment vouchers (16 percent) totaling approximately $17,000 that did not have the required approval documented by Department finance staff. For one of these three payment vouchers, we identified a discrepancy of approximately $1,000 between the vendor invoice and the receiving report included in the payment documentation. The invoice included charges for three items not listed on the receiving report. After we brought this to DPA's attention, DPA followed up with the vendor. The vendor was able to provide additional documentation showing DPA had received these three items, and therefore, no overpayment occurred. If the invoice had been properly reviewed before payment, the discrepancy between the invoice and the receiving report could have been identified and resolved by DPA prior to payment. We did not identify discrepancies with the other two payment vouchers.

It is important that all invoices are reviewed and approved prior to payment to ensure the State is only paying for goods and services actually received. DPA should ensure that staff comply with established controls over disbursements and that each invoice is thoroughly reviewed for accuracy and approved by DPA's finance office before the vendor is paid.

Recommendation No. 9:

The Department of Personnel & Administration should ensure all invoices are reviewed and approved by the Department's finance office prior to authorizing payment to the vendor.

Department of Personnel & Administration Response:

Agree. Implementation Date: Implemented.

The Department ensures all invoices contain the necessary approval documentation prior to processing payments.

Appendix

This page intentionally left blank.

Appendix

The Department of Local Affairs asked each of the nine all-hazards emergency management regions to self-assess their overall communications capabilities against 16 measures. The regions were required to assess their capabilities against the following scale: (0) "no recognition of need," (1) "recognition of need," (2) "initial efforts," (3) "moderate progress," (4) "sustained efforts," or (5) "output achieved." The 16 measures included whether:

1. Interoperable communications exists across disciplines.
2. Interoperable communications exists across jurisdictions.
3. Interoperable communications exists between state and local government.
4. Interoperable communications exists with Federal Government Responders with which first responders need to interoperate.
5. There is a formal governance structure overseeing an interoperable communications system.
6. Standard operating procedures are in place for the interoperable communications system.
7. There is a communications continuity of operations plan in place that outlines the back-up systems available at a state- and local-level as well as the protocol for use of those systems.
8. Tactical interoperable communications plans exist.
9. Agencies have operable communications systems that are in place to meet their everyday internal agency requirements.
10. Redundant interoperable communications systems are available.
11. Interoperability solution(s) are available to all first responders as authorized, without any intervention (e.g., a dispatcher is not required to make a patch).
12. A statewide set of communications standard operating procedures that conform to the National Incident Management System are in place and implemented to include operational and technical elements.
13. Plans, procedures, and use of interoperable communications equipment are regularly tested and/or exercised.
14. Personnel are trained to operate communications systems according to their roles in an incident.
15. Interoperability systems are used in pertinent everyday activities as well as emergency incidents to ensure users are familiar with the system and routinely work in concert with one another.
16. There are redundant public safety answering points that comply with phase II Federal Communications Commission requirements for cell phone access and are capable of handling a large volume of calls.

This page intentionally left blank.

The electronic version of this report is available on the Web site 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 1848