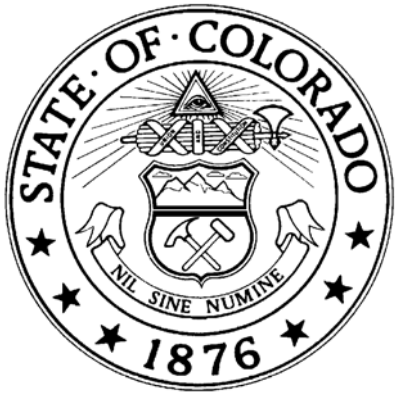

REPORT OF

THE

STATE AUDITOR

State Emergency Operations Center Computer Resources Department of Local Affairs

Performance Audit
August 2008

LEGISLATIVE AUDIT COMMITTEE
2008 MEMBERS

Representative James Kerr
Chair

Representative Dianne Primavera
Vice-Chair

Senator Jim Isgar
Representative Rosemary Marshall
Representative Frank McNulty
Senator David Schultheis
Senator Gail Schwartz
Senator Jack Taylor

Office of the State Auditor Staff

Sally Symanski
State Auditor

Cindi Stetson
Deputy State Auditor

Becky Richardson
Jonathan Trull
Reed Larsen
Rosa Olveda
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

August 1, 2008

Members of the Legislative Audit Committee:

This report contains the results of a performance audit of the State Emergency Operation Center's Computer Resources. 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. The report presents our findings, conclusions, and recommendations, and the response of the Department of Local Affairs.

Sally Symanski

This page intentionally left blank.

State Emergency Operations Center Computer Resources

Authority, Purpose, and Scope

This performance audit was conducted in response to a legislative request for an investigation into the oversight by the Colorado Department of Local Affairs (Department) of the computer equipment at the State Emergency Operations Center (SEOC) and a determination of additional safeguards needed to protect these state assets. Pursuant to Section 2-3-103, C.R.S., the State Auditor is authorized to conduct audits of all departments, institutions, and agencies of state government. The audit work was conducted in accordance with generally accepted government auditing standards and was performed from May through June 2008.

The legislative request for this audit was prompted by media reports alleging improper use of the SEOC's 30 computers. In October 2007 a Denver-based media outlet reported that the Executive Director of the Department of Local Affairs had authorized Department employees to use the SEOC computers to purchase 2007 World Series tickets. Additionally, in November 2007 the media reported that Department employees had misused the computers to surf the Internet and access pornographic and other inappropriate, nonwork-related websites. The media based its reports on its review of information for the 30 computers that media representatives obtained from the Department through a Colorado Open Records Act request.

Our audit evaluated the adequacy of the Department's controls over the SEOC's computing resources. We interviewed Department management and staff, reviewed Department documents such as information system policies and procedures, analyzed physical, technical, and administrative controls, and researched best practices and other states' policies related to use of emergency operations centers. As part of the audit we visited the SEOC, observed the facility's physical security features, accessed computers, and tested operating system, database, and application antivirus/malware utilities and Web filters. We acknowledge the management and staff at the Department of Local Affairs for their assistance during the audit.

Overall we concluded that the Department's controls over Internet access and the use of the State Emergency Operations Center's computers were somewhat lax at the time of the media reports. Since then the Department strengthened existing controls

and implemented additional controls that together provide reasonable assurance that the computer resources at the SEOC are safeguarded and available when needed. We have recommended some steps to further protect these resources.

This report contains two sections. The first section describes the SEOC and the ways in which it and its computer resources are used. The second section discusses the Department's controls over the SEOC's computer resources.

Description of the SEOC

The State Emergency Operations Center (SEOC), also known as the Multi-Agency Coordination Center (MACC), serves as the State's primary location for emergency management agencies and personnel to gather and coordinate support to local governments during a disaster or emergency. As described in the *State Emergency Operations Plan-2007*, the SEOC is "the principal point for coordinating and tasking state departments and volunteer agencies in the delivery of emergency assistance to affected jurisdictions." Additionally, the SEOC "provides the Governor with a secure location to assemble and analyze critical disaster or Homeland Security information, facilitate the decision-making process, coordinate the response activities of state government, and ensure interagency cooperation, coordination, and communications." Essentially, the SEOC is an operations center where coordination and emergency management decisions are facilitated.

The Division of Emergency Management (Division), within the Colorado Department of Local Affairs, is responsible for the management and operation of the SEOC during emergencies and nonemergencies. The Division is also responsible for assisting local government emergency management in the development and maintenance of emergency operations plans, procedures, and checklists. Division staff are not first responders (e.g., firefighters, law enforcement officers, emergency medical providers) in emergencies. First responders operate through their respective jurisdictions and are called into action through the regular local emergency mechanisms such as citizen calls to 911. One way first responders coordinate activities is through interoperable radio systems. Our October 2007 *Public Safety Radio Communications* Performance Audit evaluated statewide interoperable radio systems and discussed the use of those systems to coordinate first responders.

In contrast with first responders, the primary emergency management function of Division staff is to coordinate the acquisition, prioritization, and distribution of resources to local governments during emergency events. For example, during the January 2007 blizzard, Division staff were integrally involved in coordinating state-level assets to address local jurisdictions' needs in southeast Colorado. Among the

response efforts the Division coordinated was the air lifting of hay to stranded livestock in the region.

The SEOC is located on the second floor of the Parker-South Metro Fire & Rescue Authority's administrative office building in Centennial, Colorado. The SEOC moved from its previous location at Camp George West in Golden, Colorado, to its current location in December 2004. The SEOC includes a policy room, a secure video teleconference room, designated space for administration/logistics and planning/assessment, an operations/coordination room, and a communications center. The SEOC is equipped with 30 on-line computer workstations, three plasma screens, two smart boards, and two projection sets, among other equipment.

It is important to note that the State Emergency Operations Center facility in Centennial is not the only emergency operations center in the State. The Colorado Department of Public Health and Environment operates a similar emergency operations center as do city and county governments and private organizations. In addition, if the SEOC were to become unuseable or inaccessible, the former emergency operations center at Camp George West could be activated, because it is the designated alternate state emergency operations center location. According to Division staff, the Camp George West location is prepared in the event that emergency management personnel must gather there to conduct response efforts.

Use of the SEOC

The SEOC is used for both emergency (activations) and nonemergency purposes. According to the *State of Colorado's Emergency Operations Plan-2007*, the SEOC "becomes operational and is staffed based upon the severity of an emergency or disaster and the anticipated or actual level of involvement by state government in providing assistance to impacted local jurisdictions." During an activation federal, state, local, public, private, and volunteer agency personnel convene at the SEOC. Some of the agencies and entities that are authorized to access the SEOC during an emergency event include the:

- U.S. Departments of Defense, Energy, and Homeland Security.
- Federal Emergency Management Agency (FEMA).
- Colorado Departments of Agriculture, Human Services, Military Affairs, Labor & Employment, Public Health and Environment, Public Safety, and Transportation.
- Colorado Governor's Office.

- Governments of Colorado's cities and counties.
- American Red Cross, Civil Air Patrol, Salvation Army, and Xcel Energy.

During the two-year period of Fiscal Years 2007 and 2008, the SEOC was activated for a total of 40 days in response to six separate emergencies. These six emergencies included the holiday blizzard in December 2006, the Southeast Colorado blizzard in January 2007, the Holly tornado in March 2007, and the Weld County tornados in May 2008.

When not activated, the SEOC is used by the Department as well as other state and nonstate agencies for training (including hands-on computer training), presentations, and meetings. In Fiscal Year 2008 the SEOC was used as a training and meeting facility more than it was used as an emergency coordination center. During that fiscal year the SEOC was the site of meetings, trainings, or other events on approximately 166 days. The majority of these meetings or trainings were emergency management related and involved the Division or outside emergency management personnel or agencies (118 days). In contrast, the SEOC was activated for emergency response coordination purposes for 13 days during Fiscal Year 2008. This means that 93 percent of the time the SEOC was used during Fiscal Year 2008 (179 days), it was for nonemergencies. According to Division data, some of the groups that have used the facility for training, presentations, meetings, and emergency exercises include the:

- Colorado National Guard.
- Colorado State Managers Association.
- Joint Budget Committee.
- Tri County Health.
- American Red Cross.
- Radio Amateur Civil Emergency Service.
- State Interoperability Executive Council.

Colorado is not alone in using its emergency operations center for nonemergency purposes. We contacted managers of state emergency operations centers in five states—Arizona, Kansas, New Mexico, Utah, and Washington. We found that all five states allow emergency management related groups, such as county directors of emergency management or the National Guard, to use their emergency operations facilities for training and other purposes. Additionally, two of the five states (Kansas and Washington) allow their facilities to be used by nonemergency management groups. All five states allow these outside groups to access their respective centers' computers during trainings.

Computer Resources

The SEOC has 30 on-line computer workstations that may be used by Division staff, by emergency management personnel during activations, and by others when attending trainings at the SEOC. The workstations include standard desktop and laptop computers and printers similar to those found in other state agencies. According to Division records, at the time of our audit, the total original value of the SEOC's laptop and desktop computers, printers, and plotters was approximately $80,500. The original purchase date of the majority of this computer equipment was October 2004. Since we completed our audit fieldwork the Division has begun replacing these computers with later models.

The primary function of the 30 computers during an emergency activation at the SEOC is that they allow local government and other emergency management personnel to connect to the Internet and to access a Web-based emergency management software—WebEOC. The WebEOC software is a crisis information management system that allows users to report, track, and respond to incident reports during an emergency, disaster, or catastrophe. Using the computers, emergency management personnel can access WebEOC and share real-time information with other state, county, local, and tribal emergency management agencies. For example, personnel may use the WebEOC software and the Internet to stay current on events, locate resources throughout the state such as shelter beds or heavy equipment, and alert resource providers for possible deployment or staging within or outside of their jurisdictions.

Although the computers serve as an important tool for emergency response coordination, they are not essential to response and recovery activities. According to Department staff, the ability of emergency management personnel to meet, face-to-face, is one of the most important attributes of the SEOC. The direct physical proximity of emergency management personnel to one another facilitates communication and coordination during response and recovery efforts. This personal interface among personnel would continue in the absence of the computers. Moreover, traditional means of telephone communication and manual processes could be employed.

There are also a number of backups to accessing WebEOC and the Internet through the SEOC and its 30 computers. First, if the 30 computers were destroyed or made unavailable, other laptop or desktop computers could be connected at the SEOC to the server housing the WebEOC software and the Internet. Second, if the SEOC facility were unavailable, operations could be relocated to the Camp George West site and computers could be connected there to WebEOC. Third, authorized emergency management agencies and personnel throughout the State can, at any time, access WebEOC remotely through their own computers at their respective

locations. Finally, if the server housing WebEOC was not functioning, WebEOC could be restored because it is regularly backed-up at an offsite location.

The SEOC's computers are not directly linked to any federal, state, department, division, or local databases or systems containing sensitive, confidential, or critical information. In a prior performance audit of the Department—*Energy and Mineral Impact Grants, October 2007*—we evaluated the Department's physical and technical access controls over its primary computer system. This system houses the Department's critical applications and is hosted at a different facility than the SEOC's network. That is, the WebEOC software, for example, is not housed on the Department's primary server but at a server located at the SEOC's building in Centennial. In addition, none of the applications on the Department's primary system can be accessed by nonDepartment personnel using the SEOC's computers and none are relevant to the SEOC's operations. In that prior audit we made one recommendation to the Department to strengthen password controls and user access removal related to its primary computer system.

Controls Over Computer Resources

At the time of the media reports of improper employee use of the computers at the SEOC in the fall of 2007, the Department had a number of controls in place to safeguard the computer resources. We evaluated these controls and the events surrounding the media reports. Overall, we concluded that the Department's controls over Internet access and the appropriate use of the SEOC's computers were somewhat lax at the time the media made its reports. We found that some common controls did not exist and others that were in place were overridden or not proactively enforced. Since the fall of 2007, however, the Department has implemented additional controls and strengthened existing ones. Consequently, we concluded that the Department's current controls are appropriate and reasonable to safeguard the computer resources located at the SEOC. We have made some recommendations to the Department to further improve controls. In the following sections we describe our findings relative to the fall of 2007 and at the time of our audit work in the spring of 2008.

Control Weaknesses

A cornerstone of information security is controlling access to computer resources (data files, software, and computer-related facilities and equipment). The controls that govern system access can be physical, technical, and administrative in nature. State Cyber Security Policies issued by the Governor's Office of Cyber Security require state agencies to establish access controls that permit users to gain access to only those IT applications and systems, and to perform only those tasks on the

applications and systems that are absolutely necessary for performing their jobs. Policies also require agencies to modify access privileges when an employee's job duties change and to revoke privileges upon termination of employment. We evaluated the Department's controls that existed at the time of the media allegations of improper employee use of the SEOC's computers and found the following two areas of weakness.

Web Filtering

First, we found that at the time of the media reports, the Department did not have Web-filtering software in place to restrict users' access to certain Internet websites. In November 2007 the media reported that the SEOC's computers had been used to surf the Internet and to view personal and inappropriate, including pornographic, websites. The media based its findings on a review of Internet "cookie" reports associated with the 30 SEOC computers. Cookies are parcels of text sent by a Web server that can store information on a user's computer hard disk and later retrieve that information. The main purpose of cookies is to identify and gather information about the websites' visitors.

Cookies are not a reliable or accurate way to determine the websites that a computer user actually visited for several reasons. First, not all websites have cookies. Therefore a user could visit a particular website and there would be no cookie record of that visit. Second, some users configure their computers so that they do not accept cookies; so again there would be no cookie record. Finally, some websites have third-party cookies associated with them. For example, an organization's website could have advertisers that send cookies to users of the site even though the users never intentionally visited the advertiser's website. The cookie records, however, make no distinction between a website that was actively visited and a third-party site that the user did not access. In some cases the cookie records the media reviewed in the fall of 2007 went back as far as 2004 when the SEOC computers were purchased. The media reported that the cookie records revealed more than 30,000 hits on 3,000 websites that the media deemed to be of a personal or inappropriate nature, including pornographic sites.

As a result of the media reports, Division staff conducted a separate, detailed analysis of the Internet browser histories stored on the 30 computers. Like the cookie records used by the media, the Internet browser history records went back to the time the computers were installed in 2004. Unlike the media's review however, the Division focused its analysis on websites that users intentionally visited. Consequently, the Division's review is a more accurate reflection of user activity. On the basis of their review, Division staff concluded that users of the SEOC computers had visited 341 different websites that were "potentially" questionable. Some of the 341 websites had been visited more than once. The websites the

Division determined to be questionable included entertainment, dating/personals, pet rescue, restaurant, finance/banking, and travel websites.

We conducted a limited analysis of the Internet browser histories the Division reviewed. Consistent with the Division's findings, we did not identify any obvious pornographic websites that had been purposely accessed by users of the SEOC's computers. We also did not identify any obvious inappropriate or improper websites that the Division omitted from its list of questionable sites. Through the Division's review, the Department was able to identify the individual employees who accessed the questionable sites. The Department has decided not to discipline these individuals for the poor judgement they may have shown in the past but rather to address future Internet access issues through the implementation of additional controls discussed later in this report. It should also be noted that not all of the websites that were deemed nonwork-related or inappropriate were accessed by employees. According to the Division's study, other personnel including emergency management personnel from outside the Division and personnel using the SEOC's computers while attending training, also accessed inappropriate websites.

At the time of the media reports, users of the SEOC's computers, whether Division employees or staff from other entities, had unlimited access to Internet websites. Since that time, the Department has installed a Web-filtering software to better control and monitor user Internet access. In November 2007 the Department installed the software on its firewall that handles all of its computers including the 30 computers at the SEOC. The software allows the Department to determine which of 91 vendor-defined website categories, encompassing more than 20 million individual websites, should be blocked from user access. The Department's executive management staff determined the categories to be blocked, including: Alcohol; Criminal Activities; Dating/Social Networking; Drugs, Gruesome Content, Extreme (gory, perverse, or horrific in nature); Hate/Discrimination; Instant Messaging; Nudity; Pornography; and Violence. Some of the categories Department management chose not to block include: Art/Culture/Heritage, Business, Entertainment, Gambling Related, General News, Government/Military, Health, History, Humor/Comics, Online Shopping, Stock Trading, and Travel. According to Department management a legitimate business need either does or could exist for employees to access these and other unblocked website categories.

During our audit we tested the effectiveness of the Department's Web-filtering software by attempting to access websites containing content that should be blocked by the Department's software. Without exception, the software blocked our attempts to access these sites through the SEOC's computers. The Web-filtering software limits access to any users of the SEOC's computers. That is, the software blocks access to outside individuals attending training at the SEOC, emergency management personnel present at the SEOC during activations, and Division staff assigned to the

SEOC site. The Department has also implemented a system to monitor employee Internet use on a monthly basis by reviewing reports produced by the Web-filtering software that identifies the websites visited and those that employees attempted to visit but were blocked.

Acceptable Use Policies and Practices

The second control weakness that existed in the fall of 2007 relates to acceptable use policies. Administrative controls over access and use of computer resources typically refer to written policies, rules, and procedures. Acceptable use policies describe the authorized ways in which computer resources, including Internet and email systems, may be used by employees. On Friday, October 19, 2007 the Department's Executive Director approved the use of the SEOC's computers by Division of Emergency Management employees to purchase World Series tickets for any interested Department staff. Later the same day the Executive Director rescinded this authorization and notified employees via Department-wide email that approval was cancelled.

The Executive Director's authorization to use the SEOC's computing resources (which would have included the Internet) occurred several days before the 2007 World Series tickets were to go on sale. Therefore, no opportunity existed for staff to purchase tickets on the day the authorization was granted and subsequently rescinded. To determine whether the SEOC's computers were used to purchase tickets on the day tickets went on sale and for several days thereafter, we reviewed Internet browser information provided by the Department. We did not identify any obvious ticket websites that were accessed through the 30 computers on these days.

In keeping with the goals and requirements of the Colorado Information Security Act [Section 24-37.5-4, C.R.S.] the Department had a Cyber Security Policy that included system access and acceptable use policies at the time of the fall 2007 media reports. Among the Department's Cyber Security Policies, which became effective in July 2007, are the following:

> 13.1.9.2. Internet access is given for the convenience of staff in doing research and obtaining information in an efficient manner. Any illegal or inappropriate use of the Internet is prohibited and will be reported.
>
> 13.1.11. Users must use DOLA (Department) systems in a responsible, lawful, and ethical manner.

These policies are an integral component in the Department's overall information system internal control framework. The policies alone, however, do not ensure that

the goals of protecting the State's electronic assets against unauthorized access, misuse, or loss will be achieved. Agency management plays a key role in providing leadership and direction in this area, especially in setting and maintaining standards of compliance. As such, management must give serious consideration to any real or perceived deviation from or override of internal control policies.

At the time of our audit, the Department did not require employees hired prior to July 2007 to sign an acceptable use agreement. Additionally, the Department only requires employees to sign the agreement upon hire. The agreement stipulates that the employee is to use the computer resources for ethical business purposes only. We found that the Department needed to take steps to ensure all personnel are aware of the Department's acceptable use policy and that all current employees, regardless of their hire dates, be required to read and sign the acceptable use agreement. At the end of our audit field work, 16 of the Division's 25 employees had signed the agreement. Of the nine employees who had not signed, eight were in the field at the time and therefore, had not been available to sign the agreement. One employee, however, declined to sign the agreement. According to Department management, no disciplinary or other action is planned for this employee at this time. The Department reports that it received an informal Attorney General Opinion several years ago related to a similar situation. At that time the Attorney General's Office indicated that an employee's refusal to sign a statement was not sufficient cause for action. However, refusal to sign does not absolve the employee from knowledge of the policy or of a failure to comply. Department management indicated that any violations, whether by those signing the acceptable use policy or by an employee who declines to sign are subject to disciplinary or other action.

Nonemployee users of the SEOC computers such as emergency management personnel and individuals attending training, are also subject to comparable acceptable use agreements.

Acceptable use agreements have been used by other state agencies to help ensure employees understand their responsibilities for appropriate use of computers and computer resources. For example, the Department of Revenue requires all employees to sign a Statement of Compliance attesting that he or she has read and understands the Department's Information Technology Security Standards document and understands his or her responsibility to "safeguard the security and integrity of the Department's information and information systems." At the same time, acceptable use of computer resources by employees, including Internet and email systems, is an emerging and sensitive area for entities, particularly public sector entities. Government organizations are especially sensitive to criticism regarding the appearance of condoning or ignoring nonwork-related use of public assets especially during business hours. Some governmental agencies are beginning to address the use of computer resources in much the same way that employee use of telephones, copy

machines, faxes, and other equipment has long been addressed. It is generally accepted that employees may use their work telephone, for example, to conduct limited personal business.

The reality facing organizations today is that the computer is replacing traditional methods of communication as a primary means of conducting business. More and more businesses and government agencies are encouraging, and sometimes requiring, their customers and clients to conduct business on-line. Additionally, the use of computer systems to conduct banking transactions, make child-care arrangements, schedule medical appointments or refill prescriptions, may be more efficient than employees leaving the job site during work hours to handle these types of personal matters.

At the federal level, the Departments of Agriculture, Energy, and Justice are three agencies that have adopted policies related to employee personal use of computer resources, including the Internet and email. For example, the Department of Energy "authorizes employees to make limited use of government resources for personal purposes" when such use involves de minimus additional expense to the government and is otherwise permissible under Department rules and applicable state and federal laws and regulations. The Department of Justice allows personal use of most office equipment, including email and the Internet "where there is negligible cost to the government and no interference with official business." All three departments notify employees that they should not expect privacy while using government-provided access to the Internet or email. Additionally, employees are notified sexually explicit or illegal material is not to be accessed and violations will be subject to corrective or other disciplinary action.

Control Adequacy

Overall we believe that at the time of our audit work in May and June 2008, the Department had adequate controls in place to protect the SEOC and its computing resources. Additionally, the Department's controls provide reasonable assurance that the SEOC's computing resources will be available and functioning when needed in the event of an emergency. In addition to controls such as the Web-filtering software the Department implemented since the events of last fall, we evaluated the Department's physical, technical, and administrative controls, that were in place prior to the fall of 2007. In the following sections we describe our findings.

Physical Controls

As previously mentioned, state agencies are required to limit physical access to computer systems, networks, and data to only those authorized personnel who require access to perform assigned duties. We found that the Department's physical controls adequately protect the SEOC and its computer resources from unauthorized physical access. The Department works in cooperation with the Parker-South Metro Fire & Rescue Authority, the owner of the building housing the SEOC, to physically secure the building's perimeter and interior spaces. The building's main entrance is unlocked and open to the public during normal business hours (Monday through Friday between 7:30 A.M. and 5:00 P.M.). Physical access to the building during all other times is restricted to approved personnel through badge access. Although the building's exterior doors are unlocked during normal business hours, the interior doors leading directly into the SEOC remain locked at all times and can only be opened by authorized personnel through badge access. Physical access to the SEOC is electronically logged and monitored by a Closed-Circuit TV (CCTV) security camera system.

To test the physical security of the SEOC, we conducted several unannounced visits and attempted to gain unauthorized access. On all occasions, the doors leading to the SEOC were locked and prevented our entry. We also reviewed the list of Department employees with badge access to ensure that all were authorized by management and that all continued to have a need for such access. At the time of our audit, there were 120 individuals with badge access to the SEOC. These included 30 Department employees, 79 staff from the Department of Public Safety, and 11 staff from the Governor's Office of Homeland Security and other local public safety entities. The Department is only responsible for providing authorization for its employees and local public safety entities. The other departments are responsible for the authorization of their employees. Without exception, we found that the Department's 30 employees had approval from management for their access, remained employed by the Department, and continued to have a need for access to perform their job duties.

Technical Controls

Technical or logical controls refer to software components that manage access to computers and networks. Examples of technical controls include user IDs, passwords, and virus protection software. We evaluated the Department's technical controls and found that they are adequate, especially since the implementation of the Web-filtering software described earlier in this report. We found the following in relation to the various types of technical controls in place at the SEOC:

User IDs and Passwords. The Department had and continues to have a role-based access control model for managing a user's access to the SEOC's computer resources and networks. In a role-based model, the level of access is based on the user's role or job. The Department has established four roles or types of users who are allowed access to the SEOC's computer resources as follows:

- **Administrator.** Individuals with administrator access have the most expansive network privileges, including control over other users, network devices, and applications. For example, an administrator can add or delete users, change user privileges, disable and activate accounts, and change network device configurations. We found that access to the administrator account is appropriately limited and protected. At the time of our work, only four staff had administrator access.

- **Department Employee**. Employees with badge access to the SEOC can use their Department-assigned username and password to access the SEOC's computers. While using the SEOC's computers, Department employees may also access the Department's Local Area Network (LAN), including the general network resources, network applications, email, and the Internet using their Department passwords and user IDs. The LAN and other internal network resources are not available to the public and only limited LAN access is provided to the two types of users described below.

- **Emergency Responder.** As previously discussed, other state and local emergency responders will use the SEOC during an activation. The Department has created accounts and unique passwords for each of the 15 emergency support functions such as communications, public health, public works and engineering, and transportation. During an emergency event, Department IT staff activate the accounts. Individuals typically share the unique password assigned to their respective functions. For example, during extended emergencies, passwords will be transferred from one shift of emergency transportation responders to the next shift within that support function. Emergency responders are provided limited network access, including shared network directories, specific network applications (WebEOC), email accounts, and internet access. After an activation, the Department disables the accounts and passwords.

- **Student**. If requested by the instructor, computer access is available to groups using the SEOC for training. The Department creates a generic account and password that is shared among all students in a particular class. The Department typically disables the account after the training. The student account is the most limited of SEOC user accounts, and students generally have access only to a shared directory and the Internet.

We found the Department's role-based user access controls to be appropriate and adequate. However, during our audit, we found that the Department's password parameters are not configured to comply with State Cyber Security Policies. State Cyber Security Policies require that passwords be at least eight characters long and that they be changed every 60 days. The Department currently changes passwords every 90 days and requires only six-character passwords for the WebEOC application. Although this is not a critical weakness, the Department should comply with State Cyber Security Policies.

Malicious Software or Malware Protection. Malicious software, or malware, is designed to infiltrate or damage a computer without the owner's informed consent. Malware includes computer viruses, worms, and spyware and is most often spread through the Internet, email, and the World Wide Web. To prevent malware from infecting state computers, State Cyber Security Policies require that state agencies, at a minimum, deploy virus protection software on all computer workstations and at the email gateway, and that they configure the virus protection software to perform a full scan at least weekly. We reviewed the Department's ability to control viruses and malicious software from infecting the SEOC's computer resources and found that the Department was in compliance with State Cyber Security Policies. We found that the Department had virus protection software on the SEOC's 30 workstations and on the Department's servers, including the email gateway. Additionally, we confirmed that the Department's virus protection software was performing weekly scans and being updated for new viruses on a daily basis.

As part of our test work, we found that users can temporarily disable the virus protection software on the SEOC's computers. Disabling the virus protection software could make the SEOC's computers vulnerable to infection. To ensure all computers are adequately protected from viruses, the Department should reconfigure its virus protection software to remove this capability from individual computer users. At the end of our audit, Department staff reported that they had implemented our recommendation.

Patch Management. Hackers and other criminals typically gain unauthorized access to computers because of security vulnerabilities in software, operating systems, and network devices. To prevent cyber attacks and other unauthorized access, it is important that known software vulnerabilities are fixed or patched. State Cyber Security Policies require state agencies to ensure all operating systems and application software are kept current with vendor-issued security patches. We reviewed the Department's patch management process and found it to be compliant with State Cyber Security Policies. Specifically, the Department regularly monitors known operating system and software vulnerabilities and applies vendor-issued security patches in a timely manner.

Administrative Controls

As stated previously, administrative controls refer to the written policies, rules, and procedures that entities adopt to govern the use of computer resources. In addition to the acceptable use policies described earlier in this report, we evaluated other Department administrative controls over access to and use of the SEOC's computing resources. We found that the Department has an adequate set of computer security policies and procedures as mandated by State Cyber Security Policies. These policies address areas such as acceptable use, user account management, patch management, and computer virus and malicious software control. As part of the Department's security awareness program, all Department employees are required to attend security awareness training on an annual basis. This training includes information related to the Department's security policies and data management in addition to tips on selecting passwords. New employees are required to complete the training prior to receiving initial access to computer systems. The Department also streams acceptable use information across an electronic bulletin board in the center of the SEOC and electronically posts a notice about acceptable use on each computer when users log in.

One area in which the Department can strengthen administrative controls relates to its records of outside users who access the SEOC for training and other purposes. At the time of our audit the Division scheduled outside use of the SEOC by manually recording contact information for the organization sponsoring the meeting or training. The Department did not obtain complete information on the total number of users, such as the number of students attending training, or the names of all students present at the training. The Department should consider obtaining more complete information to better gauge the level of use of the SEOC and to more clearly identify individual users.

Overall our review did not identify fundamental weaknesses in the Department's controls in place over the computing resources located at the State Emergency Operations Center during our fieldwork in May and June 2008. However, we did identify several areas in which the Department could further strengthen existing safeguards as noted throughout this report. These areas are summarized in the following recommendation.

Recommendation No. 1:

The Department of Local Affairs should strengthen controls for safeguarding the State Emergency Operations Center's computer resources by:

a. Adopting a formal policy requiring all staff to annually read and sign the Department's Acceptable Use Agreement and monitor usage.

b. Requiring eight-character passwords for all computer resources and applications and changing user passwords every 60 days.

c. Reconfiguring its virus protection software to prevent SEOC computer users from temporarily disabling virus scans.

d. Improving the process for tracking the individuals and agencies that use the SEOC for nonemergency-related purposes.

Department of Local Affairs Response:

Agree. Implementation date: August 2008.

a. DOLA has adopted, effective August 1, 2008, a policy requiring all employees to annually read and sign the Department's Software & Acceptable Use Guidelines.

b. The eight-character password with a 60-day life cycle is also in alignment with State Cyber Security Policies requirements. DOLA will comply with this recommendation, implementing this change effective immediately.

c. The Windows firewall settings are being changed to prevent users from disabling virus scans. This will be completed by August 15, 2008.

d. The Division of Emergency Management will develop a system to better track individuals/organizations and require an attendance roster for events that utilize the SEOC for nonemergency-related purposes. This is effective August 1, 2008.

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

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

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

Report Control Number 1926