1996 ANNUAL
ILLINOIS AUDIT ADVISORY
Emerging and Potential Audit Issues

WILLIAM G. HOLLAND
AUDITOR GENERAL

Iles Park Plaza, 740 East Ash Street, Springfield, Illinois 62703-3154
Thompson Center, Suite 4-100, 100 West Randolph Street, Chicago, Illinois 60601

PHONE: 217/782-6046 FAX: 217/785-8222 TDD: 217/524-4646
E-mail: auditor@pop.state.il.us Web Site: http://www.state.il.us/auditor/audhome.htm

LAPSE PERIOD CHANGE

A new law will significantly impact the way State agencies do business. Effective January 1, 1997, Public Act 89-511 (House Bill 2251) reduces the State's "lapse period" from three to two months. Outstanding liabilities as of June 30, which are payable from expiring appropriations, must be processed no later than the close of business on August 31 rather than the current September 30.

Public Act 89-511 also requires services involving professional or artistic skills and most personal services to be actually rendered by June 30 in order to be paid from the expiring fiscal year's appropriation. Under current practices, as long as a contractual obligation is established by June 30, professional and personal services may be received during the lapse period and paid from the expiring fiscal year's appropriation.

The OAG has a home page on the Internet. The address is: **http://www.state.il.us/auditor/audhome.htm**. If you want to reach the office by electronic mail on the Internet our address is: **auditor@pop.state.il.us**.

AUDITOR GENERAL'S MESSAGE

*This is the second annual issue of the **Illinois Audit Advisory**. We initiated the **Advisory** to share information that may help agency directors, fiscal staff, and internal auditors improve agency operations.*

*Audits serve as a good source of information on potential or developing problems in State agencies. Recent audits showed that controls over State resources, such as equipment and personnel, continue to need attention. This **Advisory** contains an article summarizing findings in these and other areas.*

*The increasing prevalence of computers in State government provides agencies with the tools to become more efficient and effective. However, the use of computers creates special areas of attention for agency managers. This issue of the **Advisory** highlights some of those areas.*

*I trust this **Advisory** will provide useful information to help managers identify potential problems within their agencies so action can be taken to improve the operations of State government.*

WILLIAM G. HOLLAND
July 1996

PROTECTING STATE RESOURCES

Management has the responsibility to protect and safeguard agency resources. Such resources include property, personnel, and funds. An effective system of controls can help ensure proper use of resources.

Audits distributed by the Office of the Auditor General in 1996 may help identify areas in your agency where controls over State resources can be improved.

Property and Inventory Controls

The most common area for audit findings dealt with property and inventory controls. Audits identified several areas where improvement in property controls were needed:

- items observed were not listed on the inventory report
- items could not be located or were located at different

(Continued on page 4)

RECOMMENDATIONS TO ENHANCE COMPUTER SECURITY

Many computer users either do not understand or are unaware of accepted computer security standards and practices. As a result, information controlled by State agencies may not be adequately protected. To address this situation, State agencies should consider the following:

- **Establish a security administration function.** A clearly defined administration function can provide the necessary guidance and oversight to ensure that security objectives are achieved. These objectives should include physical security of resources, logical security of information, off-site storage of backups, and communication of security policies and issues to users.
- **Develop computer security policies and procedures.** Policies should outline the basic security guidelines and clearly identify the user's responsibility in protecting computer resources. Policies and procedures, which should be updated annually and given to all users, should include:
  - Appropriate uses of computer equipment
  - General security provisions
  - Routine backup of information
  - Off-site storage of backups
  - Systems development procedures
  - Individual responsibility to protect computer resources.
- **Establish a security awareness program.** A security awareness program should be developed to keep employees aware of security issues via memoranda, posters, electronic mail, etc.
- **Establish security standards.** In our audits of information systems, we frequently identify a general lack of standards for security. As a result, the Auditor General's Office has developed some minimum security requirements based on standard industry practices (**see inset**).

These requirements are not intended to be all inclusive and may not be appropriate in all circumstances, but serve as general guidelines that provide State government with some minimum standards for computer security.

If you have questions about computer security, please contact Bill Sampias, Director of Information Systems Audits.

RECOMMENDED COMPUTER SECURITY STANDARDS

- Each user should have an individual ID.
- Passwords should be required, have a minimum length of four characters, and be changed at least every 35 days.
- The number of times a user can log into a system after their password expires and before they change it should be limited to no more than three attempts.
- A password history should be maintained to prohibit re-use of passwords.
- After five unsuccessful attempts to enter a valid password for an ID, the ID should be revoked.
- Unless a user requires 24 hour access to a computer system, time restrictions should be set to limit when he or she can use the system.
- Users should be limited to one concurrent connection to a system.
- If a user has no activity on a system for a maximum of 60 minutes, the session should be deactivated until a valid password is entered or the user should be logged off the system.
- Access to information and resources should be limited based on the user's need and job duties.

TRAINING ON AUDITING STANDARDS

On August 1 and 2, 1996 the Office of the Auditor General will present "Professional Auditing Standards" by David Ricchiute at Brookens Auditorium at the University of Illinois at Springfield. Mr. Ricchuite is a professor at the University of Notre Dame and an acclaimed speaker on accounting and auditing.

Recently, the Office of the Auditor General sent a letter to agency directors inviting them to send representatives to this training. There will be no charge to agencies. Enrollment is limited; reservations will be taken on a first come basis.

Should your agency be interested in sending a representative to attend this course, contact Jody Middendorf, Training Administrator.

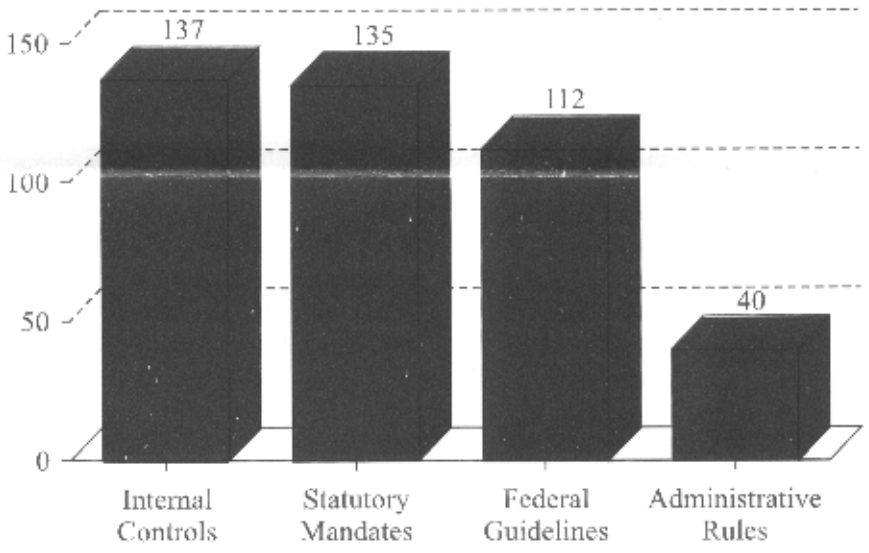
MOST COMMON TYPES OF FINDINGS

Recently released compliance audits for the fiscal year ending 1995 reported 470 findings. Most concerned internal controls (137), statutory mandates (135), federal guidelines (112), and administrative rules (40).

Over 170 findings were repeated from previous years. Recommended actions for agencies to take to address these findings included:

- Protecting State resources, such as property and equipment
- Developing effective security and disaster recovery plans for computer systems
- Keeping complete records of receipts, expenditures, receivables, property, and decision-making processes
- Improving federal cost allocation and grant monitoring.

If you have questions about these findings, contact Valerie Koch, Mandates Administrator.



E-MAIL ISSUES

The use of internal e-mail systems and Internet mail has proliferated in recent years. Many agencies use electronic mail as a primary form of communication among staff. The use of computers for communication, however, can cause significant legal problems if employees inappropriately use e-mail. Agencies may find themselves facing lawsuits alleging violations of privacy, sexual harassment, or copyright violations.

The potential liability can be staggering. In 1995, a major oil company settled a suit for over $2 million brought by 4 female employees who alleged they were sexually harassed via electronic mail.

To help protect your agency from potential litigation, specific policies regarding proper conduct online and the level of privacy users can expect need to be formulated.

ENVIRONMENTAL CONTINGENCIES

State agency operations are subject to comprehensive environmental regulation by federal, State, and local authorities. Under the federal Comprehensive Environmental Response, Compensation and Liability Act of 1980, and similar State laws, agencies are potentially liable for the cost of clean-up of various contaminated sites. During fiscal year 1995, one agency incurred approximately $121,000 in environmental clean-up costs. As of June 30, 1995 the agency had seven contaminated sites at which it may be liable for some portion of the clean-up.

State agencies should perform a periodic search for environmental contingencies in accordance with generally accepted accounting principles. Specifically, an agency should prepare and maintain a list of all potential clean-up sites and/or proceedings. For each site, an evaluation should be made at least annually to estimate an amount or range of potential total liability. This evaluation should serve as the basis for presenting disclosures of the environmental contingencies within the agency's financial statements and notes.

PROTECTING STATE RESOURCES

(Continued from page 1)

locations than listed in inventory records
- items had been traded in but were not removed from the inventory listing
- items had the wrong equipment tags
- excess inventory items existed
- access to sensitive inventory items (such as pharmaceuticals) was not adequately controlled
- annual inventory of equipment was not performed
- annual inventory certification was not filed with DCMS
- agency property control records did not agree with property records maintained at the Comptroller's Office.

Telecommunications Controls

State telephones are a vulnerable resource. An effective control system can both: 1) limit access to phones and prevent inappropriate calls from being made; and 2) identify improper calls that have been made and recoup those charges.

We identified the following telecommunications-related findings:

- no policies or procedures for telecommunications
- no reconciliation of long distance phone logs to monthly billings
- no restriction on outgoing calls
- no prompt investigation of unusual calls
- no safeguarding of credit cards and numbers.

Personnel Administration

Personnel-related expenditures are typically one of the highest expense lines in an agency's budget. As such, managers must ensure that personnel costs are effectively controlled. We found:

- uncompensated absences were incorrectly computed
- questionable unemployment claims were not challenged by the employing agency
- attendance reports did not match observed attendance
- employees were not charged for leave time used
- attendance and leave request forms were not submitted on a timely basis.

Internal Audits

The internal audit function is one of the most effective tools agency management has to ensure that an adequate system of controls exists over State resources. Audits identified that some agencies did not have an internal audit function, or that the internal auditor was not providing the minimum accepted coverage. In other agencies, internal auditors performed key operational duties which could impair his or her independence and reduce the time available to perform internal audit responsibilities.

Frequently the agencies with internal audit findings also had findings in other basic operational areas, such as inventory control or personnel administration. This suggests that a sound, thorough internal audit program is an essential component of overall effective agency management.

If you have any questions concerning these findings, please contact Tom Loobey, Director of Compliance Audits.

Recycled paper - soybean ink
Printed by Authority of The State of Illinois
LPC Order 13223 - July 1996 - 650 copies

Office of the Auditor General
State of Illinois
Iles Park Plaza, 740 E. Ash Street
Springfield, IL 62703-3154