Audit Highlights

Highlights of Legislative Auditor report on the Peace Officers' Standards and Training Commission, issued on April 20, 2009. Report # LA10-01.

Background

The Peace Officers' Standards and Training Commission (POST) became a stand alone Commission in 1999 to develop and deliver professional training, and ensure all Nevada peace officers and their agencies comply with established statutes and regulations in order to enhance the safety of residents and visitors of the state.

POST's office and training facility are located in Carson City. For fiscal year 2008, POST was authorized 17 full-time equivalent positions. The Agency's principal sources of funding are court assessments which totaled approximately $3.3 million in fiscal year 2008 and expenditures totaled about $3.1 million.

Purpose of Audit

The purpose of this audit was to determine if POST's financial and administrative activities were carried out in accordance with applicable state laws, regulations, policies and procedures. This audit included a review of POST's financial and administrative activities during fiscal year 2008. However, certain procedures were extended into fiscal year 2009.

Audit Recommendations

This report contains nine recommendations to improve POST's financial and administrative practices and its information security controls. One recommendation relates to recording expenditures properly, two relate to ensuring compliance with contracting requirements, and three relate to ensuring compliance with personnel requirements. Finally, three recommendations relate to security over POST's information systems and data.

The Commission accepted all nine audit recommendations.

Status of Recommendations

The Commission's 60-day plan for corrective action is due on July 15, 2009. In addition, the six-month report on the status of audit recommendations is due on January 15, 2010.

Peace Officers' Standards and Training Commission

Results in Brief

POST generally complied with state laws, regulations, policies and procedures significant to its financial administration. However, additional controls are needed to help ensure expenditures are recorded to the correct fiscal year, contracts are properly executed, employee evaluations are conducted, and payroll reporting requirements are complied with. In addition, POST had not developed sufficient controls to protect its sensitive information and information systems. These weaknesses included putting information system resources at risk and not implementing the state's information technology security standards. Implementing these controls will help safeguard the state's assets.

Principal Findings

Travel expenditures were not always recorded to the correct fiscal year. Specifically, out-of-state travel expenditures to attend a conference during fiscal year 2009 were improperly charged to fiscal year 2008. If these expenditures had been properly recorded, POST would have reverted $1,760 more to the General Fund in fiscal year 2008 and would have had to increase its out-of-state travel authority in fiscal year 2009.

POST paid a software vendor a total of $7,400 for two onsite software training sessions which included the instructor's related travel costs. However, written contracts were not established and thus not approved by the Clerk of the Board of Examiners as required by state law. We also noted written contracts were not prepared for services that were exempt from Board of Examiner approval. When contracts are not properly executed there is limited assurance the amounts paid are appropriate.

POST charges law enforcement agencies a registration fee for each cadet attending its basic academy training. In fiscal year 2008, POST collected about $25,000 for these fees. However, interlocal contracts establishing the scope of services provided and an agreed upon fee had not been developed. The lack of interlocal contracts increases the risk that agencies could challenge the fees charged.

POST did not complete probationary evaluations as required by state law for four of its five probationary employees during fiscal year 2008. When evaluations are not performed timely, deficiencies in performance may not be corrected timely. For one of the employees, work performance standards had not been developed, thus making it difficult to evaluate the employee's performance.

Employees that accrued compensatory time during fiscal year 2008 had not signed an agreement allowing them to do so as required by NAC 284.250. As of June 30, 2008, POST's total liability for compensatory time was approximately $3,700. When an agreement is established, employees may receive compensatory time rather than overtime pay.

POST had not established procedures to ensure employee timesheets were accurate. Two of the 24 timesheets we reviewed had notations indicating the hours worked did not agree with the hours recorded. Despite these variances, the timesheets were approved by the employees' supervisors. By not properly reviewing employees' timesheets, there is an increased risk of payroll errors occurring and not being detected.

Backup disks of POST's database containing the State's repository of peace officers' training data were not stored off-site as required by the state's information technology (IT) security standards. As a result, there is an increased risk that irreplaceable data could be lost in the event of a fire or another catastrophe.

We identified a wireless networking access point in operation in one of POST's classrooms. This wireless access point (WAP) did not have any security features enabled nor was it encrypted. As a result, there is an increased risk anyone with a laptop computer could use this WAP to connect to POST's wired network and gain unauthorized access to POST's confidential data or the State's Wide Area Network. After discussing these vulnerabilities with POST management, they took immediate corrective action.

POST had not implemented the state's information technology security standards. Specifically, POST had not conducted IT security training for existing staff or new hires and employees had not signed security awareness statements. If properly implemented, these policies and procedures can help reduce the risk that could come from unauthorized access or disruption of services.