Audit Highlights

Highlights of Legislative Auditor report on the Department of Employment, Training and Rehabilitation, Information Technology Security, issued on May 25, 2009. Report # LA10-02.

Background

The mission of the Department of Employment, Training and Rehabilitation (DETR) is to provide Nevada's businesses with access to a qualified workforce and encourage equal employment opportunities. The Department employs approximately 800 staff in its 21 office locations statewide with primary locations in Carson City, Reno, Sparks, Las Vegas, Henderson, and Elko.

The Department consists of the Director's Office and five divisions including:

- Employment Security Division
- Rehabilitation Division
- Nevada Equal Rights Commission
- Research and Analysis Bureau
- Information Development and Processing Division

The Department, especially its Employment Security Division, relies heavily on information technology and the Internet to deliver services to Nevada residents and employers. The Department stores and processes large amounts of confidential information including names and social security numbers of people working throughout the state.

Purpose of Audit

The purpose of this audit was to determine if the confidentiality, integrity, and availability of the Department's sensitive information and information systems were properly protected. This audit included a review of information technology controls at DETR through September 30, 2008.

Audit Recommendations

This audit report contains 17 recommendations to improve the information technology security at the Department of Employment, Training and Rehabilitation. These recommendations address application and access controls over the Employment Security Division's Unemployment Insurance System, data encryption, and managing user accounts. In addition, these recommendations address controls over laptop and server computers as well as wireless networks.

The Department accepted the 17 audit recommendations.

Status of Recommendations

The Department's 60-day plan for corrective action is due on August 18, 2009. In addition, the six-month report on the status of audit recommendations is due on February 18, 2010.

Information Technology Security

Department of Employment, Training and Rehabilitation

Results in Brief

Weaknesses existed in controls designed to protect the confidentiality, integrity, and availability of the Department's sensitive information and information systems. These weaknesses included: Information technology (IT) staff having unrestricted access to the State's Unemployment Insurance Trust Fund application and database; insufficient security of sensitive information downloaded onto agency laptop computers; and needing more timely removal of mainframe access of former employees. Security of magnetic tapes containing sensitive information also needs improvement.

In addition, routine network maintenance could be improved. For example, virus definitions were not current, the firewall's management needs greater attention, server rooms need better physical security, and wireless laptop security configurations should be strengthened. Finally, more effort needs to be expended to properly screen and manage network users. We noted that the Department's information technology staff either fixed or reduced the risks associated with many of the conditions we identified during the audit.

Principal Findings

DETR's Employment Security Division had access control weaknesses in its Unemployment Insurance (UI) system. Forty-seven information technology staff had either unrestricted or inappropriate user rights to the UI program and its corresponding database. This UI program is used to process unemployment claims and distribute unemployment compensation funds.

Thirty-four former DETR employees retained current access to the mainframe computer used to process the unemployment insurance transactions. These employees' access remained enabled more than 100 days after they had left DETR employment. State IT security standards require the prompt removal of users who are no longer in the Department's service.

The Department had 16 laptop computers used by DETR field auditors containing unencrypted records from employer payroll files. State IT security standards require confidential information be encrypted to prevent unauthorized disclosure if the laptop is lost or stolen.

Computer tapes containing confidential new hire data were not encrypted while being sent from employers and returned from DETR through the U.S. Postal System. Staff indicated these tapes are not erased after processing. State law requires agencies to implement reasonable security measures to protect the confidential information they collect.

Twenty-seven former employees, partners, and contractors retained access to DETR's computer network after they had left the service of the Department. State IT security standards require the prompt removal of users who are no longer in the Department's service.

The Department does not conduct routine background investigations on staff with access to IT systems or sensitive data. Background investigations are required by state information technology standards.

Sixteen of 144 computers sampled did not have current antivirus protection. The virus definition files on these computers ranged in age from 25 to 421 days old. State IT security standards require virus definition files be kept current.

DETR's internal firewall could be improved in both configuration and management. Compliance with best practices such as those issued by the Center for Internet Security will facilitate routine maintenance and administration of the firewall.

We found 16 of 32 laptops sampled did not have wireless configurations recommended by industry best practices. In addition, none of the laptop users indicated they had received security awareness training related to the risks of using wireless networking.

Four application developers had direct update access to production data on the Rehabilitation Division's primary application. By allowing application developers update access to production data, the risks of accidental or intentional corruption of the corresponding data is increased.

Network servers at 4 of the 15 locations we examined did not have adequate physical security. These servers were not secured in locked rooms in accordance with State IT security standards.

For more information about this or other Legislative Auditor reports go to: http://www.leg.state.nv.u s/audit (775) 684-6815.

Audit Division
Legislative Counsel Bureau