SUGGESTED IMPROVEMENTS IN COMPUTER CONTROLS

The Department of Employment Relations is responsible for personnel and employment relations policies and programs for state government employes. As part of its responsibility to administer the state's classified system, the Department recruits job applicants, develops and administers civil service examinations, and provides lists of qualified candidates to state agencies. The Department's operations and its 90.75 full-time equivalent employes are primarily funded from general purpose revenue, with approximately 10 percent of its budget of $6.2 million funded from program revenue generated by its training programs, publications, and services to non-state agencies during fiscal year (FY) 1997-98.

We have completed an audit of the Department as part of our responsibilities under s. 13.94, Wis. Stats. The primary focus of our audit was to review the Department's fiscal and computer operations to assess whether these activities are adequately controlled and in compliance with statutory requirements. Overall, we found the Department has appropriate fiscal policies and procedures in place, and is taking steps to prepare itself for Year 2000. However, we did identify areas in which the Department could improve controls over its computer processing.

The Department is implementing a new human resource system to replace the current systems it uses to fulfill its mission; consequently, we recognize that major changes to improve controls over the current systems may not be cost-beneficial. However, we did identify improvements the Department needs to consider implementing with its current systems: disaster recovery and business resumption planning, password parameters, and removal of log-on IDs. In addition, we note weaknesses in the areas of program change controls and access to data, which the Department needs to consider as it implements its new human resource system.

Disaster Recovery and Business Resumption Plan

A disaster recovery plan is a comprehensive framework formulated to give direction in the event of an emergency affecting computer operations. Business resumption planning involves establishing a process to resume the regular business functions of the organization affected by the disaster. Both disaster recovery and business resumption plans are critical for the continuance of any operation. Although the Department completes regular backups and off-site storage of critical data, and has informally defined the responsibilities of staff in the event of an emergency, it has not developed a formal comprehensive plan that addresses all issues related to disaster recovery and business resumption. Therefore, in the event of an emergency, the functions administered by the Department may be unavailable for a period of time.

- A formal plan is needed to ensure that the necessary steps involved in the recovery of computer processing and the resumption of operations are considered, assigned, and understood by all staff. Therefore, *we recommend the Department of Employment Relations assign a coordinator to lead the development, implementation, and communication of a formal disaster recovery and business resumption plan and to develop procedures for regularly updating and testing the plan*.

Agency Response: Once the Department has moved to its new location and completed a major upgrade to its desktop operating systems and software, it will begin working on a comprehensive disaster recovery and business resumption plan. It will appoint a disaster recovery coordinator and committee to manage the development and implementation of the plan. The committee also will be charged with meeting annually to update and test the plan. Since the Department is a small agency, it will not plan for immediate full restoration of services in the case of a disaster, but rather for a limited resumption of critical services if a disaster allows a return to normal operations within a few days or weeks.

Password Parameters

Password parameters, such as requirements to change passwords and the minimum length of a password, reduce the risk that an unauthorized user may pose as an authorized user, sign on, and access data. Once an unauthorized user has gained access, it would be difficult to detect who gained access, or even that the access had occurred. We identified a concern with the maximum days settings established for the Department's Office of Information staff.

Industry standards suggest that users change their passwords at least every 60 days, except that users with high-level access, such as access to critical information and privileges, should change their passwords every 30 days because of the higher risk their access represents. The Department has set all user log-on IDs to expire after 60 days; however, staff with high risk access, such as the administrator privilege, also have the same parameter. Therefore, *we recommend the Department of Employment Relations set the maximum days setting password parameter to expire at least every 30 days for staff with high-level access*.

Agency Response: The Department will set the maximum days setting to expire every 30 days for staff with high-level access, effective October 14, 1998.

Removal of Log-on IDs

In order to safeguard computerized data and program files from unauthorized manipulation, it is important that log-on ID records for terminated employes be suspended and removed from the system in a timely manner. Access rules for these employes must also be removed from the system to prevent possible unauthorized access and to avoid confusion and clutter on the system.

During our review of system log-on IDs, we found several outdated and suspended log-on IDs and related access rules for terminated employes, including ten log-on IDs for employes who no longer worked at the Department and seven log-on IDs that had belonged to Department of Administration staff assisting with the new human resource system. We also noted eleven current employes whose log-on IDs had been suspended by the system for non-use, which suggests that log-on IDs had been issued to employes whose specific job responsibilities did not

require use of the mainframe. Therefore, *we recommend the Department of Employment Relations delete terminated employes' suspended log-on IDs from the system as soon as practical. We also recommend the Department of Employment Relations, working with each division, regularly review job responsibilities and assess staff's need to access the Department's systems*.

Agency Response: A recently filled vacancy has been assigned the function of mainframe security officer. This person has been given the responsibility to investigate the access assigned to current suspended log-on IDs, and will be deleting IDs that are suspended or no longer needed. The security officer subsequently will review with the divisions every six months whether any staff's job responsibilities have changed in ways that would indicate removal of access.

Program Change Controls

- Computer programs often require modification as objectives and conditions change over time. Program change controls are necessary to ensure that unauthorized changes are not made to a production program. Without controls over program changes, an increased risk exists that erroneous or fraudulent changes may be made to a program.

We identified three areas of concern with the Department's controls over program changes. First, requests for program changes are not in writing or signed by an authorized individual. Formal written requests and approvals are important to document users' approval of the requested changes. Second, the same programmer is responsible for accepting a change request, changing the program, testing the changes, and moving the newly changed program back into production. Without independent review or movement of programs into production, a programmer could easily make unauthorized changes and prevent their detection. Third, program changes are not adequately documented or maintained in a central file for review or for use by subsequent programmers. Adequate documentation helps to ensure that changes can be easily identified, tracked, and understood by future programmers.

As it designs and implements its new shared human resource system, *we recommend the Department of Employment Relations establish program change procedures that require:*

- *all changes be requested by a formal, written request signed by an authorized individual;*
- *testing and approval of program changes by the user be in written form;*
- *documentation of changes be maintained for review and use by subsequent programmers;*
- *an individual other than the programmer review the completed changes to ensure agreement with requested changes. This review should be in an environment where the programmer can no longer make changes to the program; and*

- *an individual other than the programmer move the program back into production status*.

  Agency Response: The Department will immediately require that all program changes be requested by a formal, written request signed by an authorized individual and that copies of e-mail messages communicating completed changes and authorization of testing will be stored in paper files. The Department agrees that good program documentation is an important goal and is requiring proper documentation for the new shared human resource system. Changes to the programs will be properly documented and filed with the original documentation, including who requested the change, why and when it was requested, when it was implemented, and all changes to the code.

  Although the Department agrees with the goal of independent review of program changes and movement of changed programs to production, limited programming staff makes it difficult to implement. It believes that having users of the application test and sign off on the acceptability of program changes will provide sufficient review. If staff size were to increase enough in the future to make more separation of duties practical, the Department will revisit the recommendation for independent movement of programs into production.

Access to Data

Staff indicate that programmers are responsible for most of the duties related to maintenance of data. Ideally, programmers should be allowed only read access to production data, and all changes to data should be performed by the owners and users of the data. With the ability to change data, as well as extensive knowledge of the computer programs of these systems, programmers could make and conceal unauthorized changes to data. Therefore, *we recommend the Department of Employment Relations restrict access to data to only the users of the data*.

Agency Response: In its current systems, the users of data are responsible for most of the maintenance of the data. However, programmers do need update access to data in specific situations, and only as requested by the users, such as for mass corrections or updates. The new system is being designed to eliminate the need for programmers to have update access. However, in the event that a programmer does need to access the data, all changes will be audited. Any changes showing on the audit log that did not have a matching request from an authorized user will be immediately investigated.

****