STATEWIDE AUDIT

DEPARTMENT OF ADMINISTRATION--
GENERAL EDP CONTROLS

MANAGEMENT LETTER

YEAR ENDED JUNE 30, 1985

MARCH 1986

Financial Audit Division
Office of the Legislative Auditor
State of Minnesota

Veterans Service Building, Saint Paul, Minnesota 55155 ● 612/296-4708

STATE OF MINNESOTA
OFFICE OF THE LEGISLATIVE AUDITOR
VETERANS SERVICE BUILDING, ST. PAUL, MN 55155 • 612/296-4708
JAMES R. NOBLES, LEGISLATIVE AUDITOR

Ms. Sandra Hale, Commissioner
and
Ms. Nancy M. Abraham, Assistant Commissioner
Information Management Bureau

Department of Administration
208 Administration Building
St. Paul, Minnesota 55155

We have reviewed certain EDP controls for your department as a part of our statewide audit of the State of Minnesota's fiscal year 1985 financial statements and federal programs. The scope of our work was limited to the general EDP controls over the Statewide Accounting System for fiscal year 1985, including:

- organization and operation controls,
- system development and documentation controls,
- access controls, and
- data and procedural controls.

Hardware and system software controls were excluded from our scope.

We emphasize that this has not been a complete audit of all EDP controls administered by your department. Also, this work is in addition to the financial and compliance audit testing discussed in our Department of Administration Management Letter dated February 18, 1986.

The current recommendations included in this letter are presented to assist you in improving internal controls. Progress on implementing these recommendations will be reviewed during our next audit.

CURRENT FINDINGS AND RECOMMENDATIONS

The IMB Security Group should be located independently from other organizational areas and they should have an independent review of their work.

The IMB Security Group is responsible for controlling access to IMB EDP programs and data sets. They use a software security package, ACF2, in fulfilling this function.

The placement of the Security Group in an organization must take into consideration adequate authority, departmental independence, and reporting relationships. Currently, the IMB Security Group is organizationally located in the Systems Technical Support Group in Telecommunications and Technology Management. They are in a software support area under several levels of management. We feel that there could be an independence problem with the Security Group being located in a software development area. We have also found that there were people working in the software support area that have the clearance to write access rules (security officer status in ACF2). This clearance should be limited to the Security Group and necessary backup personnel. Finally, the Security Group is not at at level in the organization that is high enough to provide for adequate authority. They must have the authority to deny unauthorized access to files and programs and to address other security issues. We feel that it could be difficult for them to deny access to someone who is organizationally above them.

The IMB Data Security group monitors ACF2 security violation attempts and notifies the supervisor of the person that caused the violation attempt if it is felt to be significant. The Security Group also writes access rules for the programs and files and creates logonids. They are thus in the position of writing access rules and monitoring violations. Rule writing and violation follow-up are activities that are not regularly reviewed by an outside party. This situation could allow errors and ommissions to go unnoticed.

RECOMMENDATIONS:

1. *The Data Security Group should be in a organizational position separate from a software development area. The Data Security Group should be at a level high enough in the organization to maintain independence in dealing with granting access and other security issues.*

2. *A regular independent review of access rule changes and violation attempt follow-ups should be performed by someone outside of the IMB Security Group.*

<u>User agencies sometimes fail to provide the IMB Security Group with sufficient documentation</u>.

Access to the computer system is controlled through the use of logonids and their corresponding passwords. Logonids identify the user to the system and passwords signify that authorization is granted. User agencies sometimes need a logonid change to enable a person to have access to the system when they have forgotten their password. This change typically results from telephone conversations between the Data Security Group, the user, and the user's supervisor. The user is frequently questioned over the phone to provide identification. This procedure results in no supporting documentation. Rule modifications are also made verbally in some cases if changes are needed urgently. In these cases, user agencies are sometimes slow to send documentation or fail to send it entirely. The absence of documentation creates the possibility of errors and misunderstandings. It also leaves the burden of support for changes on the IMB Data Security Group. A daily log of verbal authorizations for rule and logonid changes would be a helpful tool to ensure the receipt of written documentation.

In addition, the responsibility for requesting the IMB Data Security Group to cancel or suspend a person's logonid rests with the user agency. There have been instances where agencies have not notified the Security Group of employees that have left or changed employment. If such an employee's logonid is not cancelled or suspended, an unauthorized and possibly disgruntled person would have access to the system. The Department of Finance has a system for identifying users of the Statewide Accounting System that have changed employment. The IMB Security Group is using that information and consequently covers a large number of logonids. However, the IMB Security Group does grant logonids which are not governed by the controls imposed by the Department of Finance. We believe that IMB should exert additional control over these logonids. For example, there could be a report that matches employment records to logonid records and lists those that have changed employment. If such a report is not feasible, agencies should be reminded regularly of their duty to report employees that have changed employment.

RECOMMENDATION:

3. *The IMB Data Security Group should obtain written documentation to support all modifications to logonids and rules, including those granted through verbal authorizations.*

4. *The IMB Data Security Group should strengthen procedures for identifying employees with active logonids that have left or changed employment.*

The UCC7 job scheduling package operates outside of the ACF2 security system.

UCC7 is the job scheduling package that handles production jobs such as the daily Statewide Accounting System. For example, the daily expenditure transactions are processed each night using this system. ACF2 is the access control facility which provides protection for the system's files and programs by comparing a person's user identification string with authorization rules for the program or file. The company supplying UCC7 and the company supplying ACF2 have not worked together to make the UCC7 software package function within the ACF2 control system. Since UCC7 operates outside of the ACF2 system, a person with access to UCC7 on a UCC7 terminal can access any file or program regardless of the ACF2 access rules. Thus, it would be possible for programs or files to be altered without authorization and without being reported by ACF2. There have been software modifications that have been developed by other users of ACF2 that enable it to provide access control for the UCC7 system. These software modifications are available to others, but they may have the drawback of being difficult to install and support because the supplier does not support software it does not develop.

If IMB determines that a software modification is not feasible at this time, alternative access controls over the UCC7 terminals should be considered. Currently, the UCC7 terminals may be freely accessed by any of their numerous users. No record of UCC7 terminal usage is kept. Controls over the UCC7 terminals would be improved if physical access to the terminals was limited and activity was logged.

RECOMMENDATION:

5. *The Information Management Bureau should evaluate software modifications that enable ACF2 to provide access control protection for the UCC7 package. If it is not feasible to implement a software modification, alternative access controls should be implemented.*

<u>The control over system output needs improvement</u>.

Output that is printed centrally at IMB is either put on shelves for pick up at the user agency window or put on a table for pick up by those allowed access to the IMB floor. Both means of distributing output could be improved. The current distribution methods are vulnerable to having output misplaced or stolen. Also, output will often contain confidential information which deserves extra protection.

The output for external agencies is grouped by agency or shelved. There is no ID check for the person picking it up. Access to output is unlimited and unmonitored. There is also no signature required for output received. This system could be improved by having someone check for authorization to pick up output and having the person who picks it up sign for it. Courier delivery of output to agencies would improve controls as well. Another alternative would be a lockbox system in which output is grouped by agency in boxes which can only be accessed by an authorized person with a key or combination.

The output generated internally by those having access to the IMB floor is unprotected and can be browsed or taken by anyone having access to the floor. An improvement would be to have the output delivered to the authorized person's work area rather than the output table.

RECOMMENDATION:

6. *There should be an improved system for giving output to authorized people.*

Thank you for the cooperation extended to our staff during this audit.

James R. Nobles
Legislative Auditor

John Asmussen

John Asmussen, CPA
Deputy Legislative Auditor

March 11, 1986

SF-00006-03

STATE OF MINNESOTA

Office Memorandum

DEPARTMENT OF ADMINISTRATION

TO: John Asmussen
Deputy Legislative Auditor

DATE: March 11, 1986

FROM: Sandra J. Hale, Commissioner
Nancy M. Abraham, Assistant Commissioner

Nancy Abraham

PHONE: 296-8083

SUBJECT: Management Letter

We appreciate the opportunity to review and comment on the preliminary draft of your management letter regarding your EDP audit of the general controls over the Statewide Accounting System. The assistance you provided through this audit will prove helpful to the department as we continue to improve our EDP operational controls.

We have numbered our responses to correspond to your recommendations. Our responses outline what we have done or propose to do to implement your recommendations.

1. The Data Security Group will be moved to an organizational position separate from the software development area. It will be placed at a high enough level in the organization to maintain independence. Nancy Abraham is the person responsible.

2. Periodic and random, independent reviews will be performed of access rule changes and violation attempt follow-ups by someone outside of the IMB Security Group. Nancy Abraham is the person responsible.

3. A log of verbal LOGONID changes is now being maintained. It contains the LOGONID, requestor, change, changer, and a comments column. When a verbal rule change is requested, the Data Security Group fills out and files the proper form, noting the source of the request. When the written documentation is submitted by the agency it is attached to the appropriate form and refiled.

   If the agency does not submit their written documentation within one week, the Security Group will follow-up with a written reminder to them. The agency will be advised that if the Security Group doesn't receive the documentation within two more weeks their LOGONID will revert to its original form. Howard Tri is the person responsible.

4. Strengthened procedures for identifying employees with active LOGONID'S that have left or changed employment will be developed with the Department of Finance. This will involve some changes to the state payroll system. Howard Tri is the person responsible.

5. Software modifications that enable ACF2 to provide access control for the UCC7 package will be implemented. Since neither the ACF2 nor the UCC7 vendor actively supports such a modification, but merely offers software exit points, this modification must be carefully evaluated and planned. Howard Tri is the person responsible.

6. An improved system for distributing output to authorized people will be implemented as part of the redesign and relocation of the IMB Production Control Group on the fifth floor of the Centennial Building. Plans for handling output will be reviewed with audit staff before construction plans are approved. Dick Kelly is the person responsible.

Thank you, again, for the assistance your staff provided in this audit.

SJH/MNA:cg