LOCAL COMMISSIONERS MEMORANDUM

DSS-4037EL (Rev. 9/89)

Transmittal No: 91 LCM-85

Date: May 8, 1991

Division: Information Technology Management

TO: Local District Commissioners

SUBJECT: Security Investigations

ATTACHMENTS: None

The strengthening of Data access security is a continuing goal of the Department of Social Services. Recently, the Department adopted a comprehensive data security policy which was incorporated in the Local District Managers Guide. Maximizing security controls is predicated on the ability to track the identity of individuals who use on-line systems. For this reason, an important cornerstone of the system is to give each person a single unique user identification (userid). This gives us the capability to know who signed on to a terminal to begin an on-line session.

In conjunction with this, the Department Security Committee has approved Mainframe Security Rules which document the requirement to log access attempts to database information. These audit log files identify what transactions were run during a terminal session, providing us with the ability to reproduce certain information concerning data access. In the future, to supplement this capability, we plan to identify what case was inquired against or updated by each transaction.

In the past, we have occasionally been requested to provide this type of information to a County Commissioner or HRA. This information is normally requested in order to support a security investigation. In order for us to initiate any work on your request, as much of the following data as is available should be provided:

- Date and time of terminal session
- PID number and Site identification (Siteid) of the device
- Transaction used
- Userid involved

Our ability to provide you with useful information is dependent on having as much of the above data as possible and as precise as it can be described.

The stored audit information is voluminous and is therefore required to be kept on a limited retention basis. Therefore, it is essential that we are informed of your needs and the date of the data you are requesting as close to the event as possible. This will enable us to place a hold on audit information that may otherwise be lost. After approximately two weeks, detailed information such as transaction updates to a case may not be available and our ability to satisfy your request diminishes.

Several types of data can be gathered for your use. If a transaction is identified, we can provide all userids that accessed that transaction for a particular day or days with the terminal on which it was attempted. If necessary, an ID can be tracked to determine what transactions were attempted by it for a specified time period, such as a particular day.

Each security investigation request must be in writing from the county Commissioner or HRA Inspector General to the Director of the Bureau of Data Administration. A contact person familiar with the request should be identified in your transmittal and it is advisable that an advance phone call to TTSS Operations (518-473-5755) be made. We will confirm your request within seven business days of the date the request is received. In general, our response will take 2 to 4 weeks to complete.

If we receive a contact from anyone in your organization that appears to involve a security breech, we will take steps to notify you. This action will be taken to ensure you are fully aware of these matters. If you have any questions, please contact Jerry Kristie at (518) 473-5755.

Sincerely,

Allan R. Goldsmith
Director,
Bureau of Data Administration

ARG:kg