UNIT ORDER #46 - SECURING EMPLOYEE ELECTRONIC MAIL

PURPOSE OF THIS ORDER:

Since the Department's Electronic mail system (email) is a daily source of communication between our employees, information contained in the email system may contain evidence that is important to investigators. To ensure that the evidence is not lost, the investigator should seek to suspend the employee's access to the email system when there are allegations of systems misuse or when the employee becomes the subject of a criminal or administrative investigation wherein securing the email system may have evidentiary value to the investigator.

SCOPE:

To ensure that the evidence is not lost, the investigator or the person taking the notification that an employee is suspected of email abuse or when the employee has been relieved of duty, should notify the Sheriff's Data Network and request that the employee be locked out of the system. During normal business hours, the request should be made to the Data Systems Bureau (DSB) Operations Lieutenant. After hours, the request should be made to the on-call NT administrator, in care of the JDIC Help Desk at (323) 267-2064.

Locking the employee out of the system can be either permanent or temporary based on the focus of the investigation. Locking the subject out of the system will allow Data Systems Bureau to isolate the employee's records before the employee's access rights are restored. Consideration should be given to immediately taking/securing the actual machine the employee was using in case information was saved locally.

DUTIES AND RESPONSIBILITIES:

The Data Systems Network Manager can be notified seven days a week. Normal requests for email information should be sent to the DSB, in care of the Operations Lieutenant, by email or memorandum.

DATA SYSTEMS BUREAU:

Due to the growing demands on the "**server resources**" managed by the DSB, they have instituted a policy to purge employee email that was restored for administrative investigations. Beginning in May 2002, during the first week of each month, DSB will delete any secure folders which were created more than six months prior (e.g. in May, they will delete all folders created before the previous October).

If email is needed for a particular investigation beyond six months from the date of restoration, the investigator is responsible for contacting DSB to request an extension. In that case, the investigator must provide DSB with the identification number of the secured folder(s).

During the last week of each month, DSB will notify the investigator which folders are scheduled for deletion. This will give investigators ample time to determine if there is a continued need for DSB to retain the secured folders

If an extension is not requested through DSB the information will be purged and the process for retrieval must be reinitiated by the investigator.