


**Collier County
Clerk of the Circuit Court
Internal Audit Department**

Management Advisory 2000 - 1

To: Dwight E. Brock, Clerk of the Circuit Court
From: Robert W. Byrne, CMA Internal Audit Director 
CC: Audit File
Date: 12/23/99
Re: Interim Review of MGSI Security Procedures

MGSI DATA SECURITY REVIEW

BACKGROUND

The Internal Audit Department has completed an interim review of MGSI security procedures and access restrictions. The audit covered the period of May 1999 - November 1999. Previously, Internal Audit had conducted weekly tests of access restrictions but this practice was discontinued because no exceptions were found and the area under review was assigned a low risk. Due to staff turnover, the Internal Audit Department determined that it should test those assumptions and therefore initiated this interim review.

The MGSI system (Moore Governmental Systems Inc.) has been in use since 1988. Security procedures are governed by the "MGSI Data Security Procedures Manual" which lists the methods for obtaining proper authorizations and access to the various applications. The Request for Electronic Information Access form (REIA) is the vehicle for providing the various levels of approval and purpose for accessing information.

The purpose of this memorandum is to communicate the objective and scope of our review and to inform you of our audit findings and recommendations.

AUDIT OBJECTIVES & SCOPE

The objectives of the MGSI Data Security Review were to determine whether existing procedures are adequate for controlling:

- (i) ID/password administration and changes
- (ii) Additions, deletions, and changes to data access security.

We reviewed the existing "MGSI Data Security Procedures Manual" and "MGSI Security Data Entry Instructions". We interviewed security administrators, senior systems analyst and users. We sampled

and tested additions, changes and deletions to MGSi security access. We examined ID's and passwords and tested current system access for authorization.

FINDINGS

Listed below are our findings:

1. The "MGSi Data Security Procedures Manual" has not been formalized to ensure that security administration complies with the desires of the Clerk of the Circuit Court.
2. Our examination revealed that some passwords consist of the user's name or of a similarly easily guessed value.
3. Individuals no longer employed by Collier County Government continue to have ID's on the system. (A sample of 20 ID's revealed that 11 had not been deleted from the system.)
4. Cloned profiles did not have supporting documentation for access restrictions.
5. Passwords were not encrypted and were printed on reports.

RECOMMENDATIONS:

Following are our recommendations corresponding to the above findings that were discussed with management. Management responses to the recommendations are included in italics:

1. The "MGSi Data Security Procedures Manual" should be formalized.

Formalization of the "MGSi Data Security Procedures Manual" has been added to the Security Administrator's current year work plan.

2. The current password standard only requires that passwords be a certain length. The standard should be re-written to include the following:
 - passwords should be a combination of alpha and numeric characters
 - passwords should not be identifiable with the user (such as first name, last name, spouse's name, pet's name, etc.).

In the future, the Security Administrator will require passwords to include both letters and numbers.

3. As part of personnel exit procedures, we recommend that a document requesting system ID deletion be forwarded to the Security Administrator.

A procedure to remove terminated employees VMS ID's has previously been implemented and will be expanded to include deleting MGSi ID's as well.

4. A procedure for documenting cloned profiles should be established so that documentation of access restrictions exists for all ID's.

A procedure for printing access restriction documentation from the system and attaching it to cloned profiles has been implemented.

5. Passwords should not be displayed on the computer screen when entered or on printed reports.

MGSI does not encrypt passwords. Any new system should include one way encryption of passwords. A request to remove passwords from security reports has been submitted to MIS.

CONCLUSION

While system security requires constant vigilance, the Internal Audit Department believes that with current procedures and with implementation of the above recommendations, there is a minimal exposure to risk from a security standpoint within MGSI. The Internal Audit Department will continue with MGSI security reviews appropriate to this level of risk.

The Internal Audit Department would like to thank Jim Mitchell and Shirley Van Vliet of the Finance & Accounting Department and Dave Witham, James Taylor, and Judy Stephenson of the MIS Department for their cooperation and assistance in this review.