U.S. Department of Housing and Urban Development
Office of Inspector General
451 7th St., S.W
Washington, D.C. 20410

MEMORANDUM NO:
2003-DP-0802

December 3, 2002

MEMORANDUM FOR: Michael Najjum, Jr., Senior Vice President, Office of Finance, TF

//SIGNED//
FROM: Curtis Hagan, Director, IS Audit Division, GAA

SUBJECT: Review of General Information Technology Controls at ACS

INTRODUCTION

This memorandum provides the results of our limited review of the general controls over the information systems operated and maintained for Ginnie Mae by Affiliated Computer Services – Governmental Services, Inc. (ACS). Our review was made in response to a request from Ginnie Mae. This memorandum provides the results of our limited survey work of the general controls at ACS.

Our review found that security over certain server and application access controls can be improved. We also found that required semiannual testing of the disaster recovery process for one (the webserver) of the three major ACS contracted services was not being performed. We have made five recommendations to Ginnie Mae to improve internal controls in these areas.

We conducted an exit conference on July 26, 2002, with ACS officials regarding our review. We also received written responses by ACS on an email draft of our preliminary findings and on the draft of this Memorandum. Their comments and our response thereto are included in the Results of Review section of this memorandum. We also conducted an exit conference with Ginnie Mae officials on November 4, 2002. They expressed agreement with our findings and recommendations.

Within 60 days, please submit for each recommendation a status report on: (1) corrective action taken; (2) the proposed corrective action and target completion dates; or (3) why corrective action is considered unnecessary.

BACKGROUND

Through its Mortgage Backed Securities (MBS) pools programs, Ginnie Mae provides increased availability of reasonable cost residential and other mortgage loans by guaranteeing investors of pool securities their scheduled principal and interest payments in case of default by either the issuers or borrowers. Ginnie Mae has contracted MBS transaction and record keeping functions out to two primary contractors – Chase and ACS. Chase serves as the Central Paying and Transfer Agent, which sends the mortgage payments and guarantee fees received from the issuers to the investors and Ginnie Mae, respectively. ACS receives monthly and quarterly accounting reports from the issuers and Chase, which are used for reviewing, analyzing, and reconciling the mortgage cash flows and principal balances to the remaining security pool investment balances. ACS also reconciles guarantee fee payments collected and paid over to Ginnie Mae. In addition to these services, ACS performs risk analysis of mortgage pool information, monitors compliance with Ginnie Mae's custodial bank ratings, processes requests for Soldiers' and Sailors' loan qualifications and reimbursements, and performs special reviews related to the MBS programs. To conduct this work, ACS is responsible for administering Ginnie Mae hardware and software systems (including the Ginnie Mae Business Center and the local and wide area networks). It is also responsible for supplying other hardware, and for designing and implementing software enhancements and system interfaces as needed.

METHODOLOGY AND SCOPE

Our survey reviewed: (1) security over server and application access (including server access methods, file and directory access rights and the password file), and Oracle database access via the web-based server; and (2) server back-up and disaster recovery plans. We selected three UNIX servers for review (ARMBSIS1, ARMBSIS2, and GNMABC1). The first two servers are used for the Mortgage-Backed Securities Information System (MBSIS) application, which contains the monthly reporting information from the MBS issurers and Chase. These two servers are located at ACS facility. The GNMABC1 server is is located at the Ginnie Mae Business Center and is used for Ginnie Mae's database applications, accessed via a webserver.

Our review methodology included testing controls over system directories and files by obtaining server access (no administrative privileges), and issuing system commands. We obtained a list of ports available on the server from the system administrator to determine whether certain ports represented a security risk. We also determined whether outside parties could telnet to these servers from an external network. We interviewed the database administrator for the Oracle databases to determine whether access to these databases were properly controlled. We requested and reviewed the procedures for the backup and disaster recovery plans. Our survey work was conducted from April 19 through July 26, 2002.

For the fiscal year periods June 30 of 2000 and 2001, ACS's Ginnie Mae operations were reviewed by a contracted CPA firm. The CPA firm reported in November 2001 that all information system issues observed in the current and prior years have been corrected or resolved.

RESULTS OF REVIEW

On July 3, 2002, we provided the preliminary results of our survey to ACS and GNMA via an email. We conducted an exit conference on July 26 and certain follow-up discussions with ACS staff regarding those results. The following issues regarding server/application access and server backup/recovery remain unresolved and we are making recommendations for their correction.

Server/Application Access

Directory Access. Our review found that the owners of the system directories of the ARMBSIS1 and ARMBSIS2 servers were appropriately established. However, the owner of a system directory (generally referred to as the "home" directory) for the GNMABC1 server was set to an individual user. Ownership of this directory could provide that user with unauthorized access to other users subdirectories and files.

The system administrator could not explain how the owner of the "home" directory of the subject server was set to an individual user. The system administrator said the issue is a mute point now because that server is now the backup server, and he had removed the individual as the "home" directory owner.

To help ensure that ownership of the system directories are properly controlled in the future, we recommend that GNMA require a periodic security listing of directory owners. Although this requirement is a passive control, it would encourage ACS to resolve these issues prior to submitting the security listing.

Telnet Access to GNMABC1. We tested the telnet access method to the three servers to determine if the connections were open to external parties. We were unable to obtain a connection to the two MBSIS application servers located at ACS in Maryland, but GNMABC1 server at the HUD Business Center in Washington DC was open. If connections are available, cracker programs could be used to guess the password. Subsequently, we tried the connection, but were unable to connect. During the exit conference, ACS explained that they needed the telnet access for maintenance purposes but they could not explain why we could no longer connect. The ACS staff did say that HUD can restrict telnet access to certain IP addresses and we do recommend that this be done.

Unneeded Server Port Services. Our review found that certain server ports with various miscellaneous server commands were enabled. For example, internet ports using server command executables, such as, "chargen", "whois" and "finger" user identification programs, "pop" and "pop3" mail programs, "portmap", and "exec" were available. These ports and services could be exploited. We could not identify a need for these services. Therefore, if these services are not needed, the ports should be disabled.

During the exit conference, ACS stated that these ports and services have since been disabled. We consider this issue closed and therefore, we are not making any recommendations in this area.

Access to the Oracle Databases. The ACS administrator for the Oracle databases residing on the GNMABC1 server informed us that Oracle's built-in security component is not being used to control access and encrypt the passwords to the databases. Access to database records is gained through other applications that link to the databases. Although user passwords over a secure Internet protocol are required to access these applications, those passwords are being stored in clear text on the Oracle database and represent a security risk.

In its written response to our preliminary security issues, ACS stated: "We believe that there is no real risk of breach of security for these user ids and passwords. However, as a technical consideration, the use of Oracle encryption would increase the security features. Making the suggested change requires Ginnie Mae approval. The change does require modifications to the design and coding of the Web EDI and GMECS applications."

We recommend that Ginnie Mae conduct a study to determine the best solution to improve the database security. This study should consider ACS suggestions mentioned above, but also consider additional or other solutions, such as upgrading the older Oracle software versions to include the Oracle Advanced Security Option with X.509 security certificates (available on Oracle version 8 and above).

Server Backup/Recovery

Backup Procedures. Our review found that ACS' procedures for backing/restoring system files and application data were adequate and were being followed. ACS performs full system backup daily, and the backups are kept for 5 weeks at the offsite location located more than 60 miles from the ACS processing center.

Disaster Recovery Procedures. ACS has established disaster recovery plans, which require semiannual testing for each of the three major IT functional areas – the MBSIS databases, EDI (Electronic Data Interchange processing), and the web server. We found that semiannual testing was being performed for the first two functional areas, but not for the web server.

ACS has three servers setup for the Ginnie Mae website. The main (production) server and the backup server are both located at the Ginnie Mae Business Center. ACS has established the backup server as a "mirror" of the production server with replication of the server's website and certain Oracle databases. Load balancing of server requests have been established between the two and if the production server goes down, website visitors will automatically be switched (fail-over) over to the backup server.

The disaster recovery web server is located at another contractor's site (UUnet). Although the production server's website is replicated on the recovery server, the Oracle databases are not. In addition, there is no automatic fail-over to this server if both of the servers at the Business Center go down. Because automatic fail-over has not been established, ACS did not perform the disaster recovery testing for the Web Site. It estimated it could take up to six days to transfer the domain name (GinnieMae.gov) to and from the recovery server and to propagate the changes throughout the Internet. ACS felt that a possible six days of service interruptions are not acceptable in an enterprise web environment.

From a review of various products on the Internet, we found there are several software, hardware, or a combination of both solutions for establishing an automatic fail-over of the website procedure to the recovery server regardless of the location of the servers. These solutions range from relatively simple to more complex. If desired, Ginnie Mae might want a continual polling of the production and backup servers to see if they are in operation with an automatic switch over to the recovery server if they are not. The recovery server can be included in the load balancing scheme if deemed necessary. The website file changes can also be backed up on the recovery server in real-time or less frequently. ACS or Ginnie Mae's current hardware (servers or routers) or software vendors may also offer similar solutions. We recommend that Ginnie Mae study the different alternatives in order to implement an efficient automatic fail-over solution for the disaster recovery of the website.

The ACS disaster recovery plan for the web server did not include recovery or linking to some of the other web services, including the production server's Oracle databases, because these services were not connected or replicated. We recommend that Ginnie Mae consider including these other resources in the web server disaster plan through use of the above suggested cluster techniques.

RECOMMENDATIONS

We recommend that Ginnie Mae:

1. Request that the HUD IT Office restrict telnet access to only those IP addresses needed by ACS.

2. Require a periodic security listing of directory owners to ensure that directory ownership is proper.

3. Conduct a study to determine the best solution to improve the security of Oracle databases, linked to the webserver.

4. Implement an efficient automatic fail-over solution for the disaster recovery of the website.

5. Conduct a study to determine the cost-benefits of including webserver related databases and applications in the disaster recovery fail-over solution.

DISTRIBUTION OUTSIDE OF HUD

The Honorable Joseph Lieberman, Chairman, Committee on Government Affairs
The Honorable Fred Thompson, Ranking Member, Committee on Governmental Affairs
Sharon Pinkerton, Senior Advisor, Subcommittee on Criminal Justice, Drug Policy & Human Resources
Andy Cochran, House Committee on Financial Services
Clinton C. Jones, Senior Counsel, Committee on Financial Services
Kay Gibbs, Committee on Financial Services
Stanley Czerwinski, Director, Housing and Telecommunications Issues, U.S. GAO
Steve Redburn, Chief Housing Branch, Office of Management and Budget
Linda Halliday, Department of Veterans Affairs, Office of Inspector General
George Reeb, Assistant Inspector General for Health Care Financing Audits
The Honorable Dan Burton, Chairman, Committee on Government Reform
The Honorable Henry A. Waxman, Ranking Member, Committee on Government Reform