State Auditor's Office

John Keel, CPA
State Auditor

An Audit Report on

Financial System Controls at the University of Houston

November 10, 2005

Members of the Legislative Audit Committee:

Security controls within the University of Houston's (University) financial system are adequate to protect critical data from unauthorized alteration, loss, or improper use, but further improvements are necessary. The University has enhanced its financial system's security by implementing prior audit recommendations. However, the University can further improve security controls to protect critical data by (1) limiting direct database and high-level user access and (2) logging and monitoring application and database access.

In addition, although the University's financial system controls are effective in ensuring that financial data and reports are materially accurate, certain improvements should be made in classifying purchases, reporting accounts payable, and enhancing financial system input controls and audit trails.

The University can increase the effectiveness of access security controls in its network and in its financial system application, database, and operations.

Improving the configuration of information resources. Information resources are vital assets that should be protected. Proper configuration of networks can provide important and invaluable protection against unauthorized access, modification, or destruction of these resources. At the University:

- The Web-based financial system was accessible from the Internet outside of the University's network at the beginning of this audit. However, the University successfully disabled the connection after auditors identified it. This unnecessarily exposed the University's resources to unauthorized access and could have had serious, adverse results if it had not been addressed.

- Auditors identified another issue that increases the risk of unauthorized access to the University's financial system. To minimize the risk associated with public disclosure, this report does not identify the specific vulnerability because doing so could further jeopardize the security of the financial system. Auditors have provided the University with detailed information describing the vulnerability and a recommendation for correcting it.

Recommendations

The University should:

- Ensure that the financial system can be accessed only from within the University's network.

- Address the specific vulnerability that was communicated separately to improve the security of the financial system.

Controlling access to the financial system. Access to the University's financial system (in particular, the part of the financial system that users see on their computer screens) is controlled by the assignment of unique IDs and passwords. Each user is assigned roles with access rights necessary to perform his or her duties. In reviewing the configuration of the financial system, auditors identified the following:

- The University does not monitor logs generated by the financial system to identify patterns of unauthorized access. These logs record who accessed the system, from what location, and when they logged in and logged out. Without regular monitoring of these logs, the University may not detect or be able to prevent unauthorized access.
- The University's controls over user accounts and passwords in the financial system application allowed seven user accounts to remain enabled when they should have been disabled. One user account was still enabled more than six months after the last login, which is contrary to University policy, and six remained enabled after the application should have automatically disabled them. The University has an adequate security policy and has made significant improvement since the last State Auditor's Office audit in November 2004 (see *An Audit Report on the Protection of Confidential Information and Critical Systems at the University of Houston*, SAO Report No. 05-010). However, because user accounts are not always disabled when they should be, inappropriate users—those with no legitimate reason to access the financial system—have the ability to alter or improperly use financial information.
- The University had successfully disabled all but one of the financial system's default user accounts, which are included in the standard installation of the financial system and are typically not assigned to individual users, and it removed the access rights of the remaining account after auditors identified it. The one remaining default account was not fully disabled because it is needed by the financial system. Removing the access rights prevents users from using the system through this account instead of through their own unique accounts. Before the University removed its access rights, this account had access to all functionality in the financial system. This access could have allowed users to, for example, submit and approve payments to themselves. Title 1, Texas Administrative Code, Section 202.75(3)(A), requires that all users of information resources be assigned unique identifiers and use their identifiers to gain access to applications.

  Furthermore, before the remaining account's rights were removed but during this audit, the lead database administrator used it to access the financial system. This gave this individual complete control over the application and the database, which could have been used to process any transaction without detection.
- Security roles, which grant users certain rights within the financial system, are not defined or documented. Documentation of security roles is necessary to prevent accidental or inappropriate authorization of access to the financial system and to ensure efficient business continuity.
- A single individual holds the positions of Director of Financial Systems and Security Administrator. As a result, this individual could assign a user the authority to create transactions and then change those transactions at a later time without supervisory review or approval. An effective control structure would segregate these two critical functions.

Recommendations

The University should:

- Regularly monitor the financial system access logs and follow up on any issues noted through monitoring.

- Ensure that all accounts that have not been accessed within six months are disabled, in accordance with University policy.

- Determine the cause for the automated application security errors and correct them.

- Prevent unnecessary user accounts from having access to the financial system, either by disabling accounts or removing all access rights to default user accounts that must be kept enabled.

- Define and document descriptions of the security roles in the financial system.

- Separate the functions of Director of Financial Systems and Security Administrator.

Controlling access to the database. The University's financial system uses a database to store the data that is displayed to users of the financial application. A good system of controls would (1) ensure that only database administrators have direct access to the database for normal maintenance (such as installing upgrades and patches) and (2) require database administrators to access the database through the use of unique identifiers with strong passwords. Application users should not have direct access to the database. At the University:

- Controls over one account with extensive access to the database are not sufficient. This account is necessary for the application to function and must be used by database administrators to install patches and upgrades. However:

  - Responsibility for this account is not assigned to a specific individual.

  - The password for this account is shared among the database administrators.

  Sharing account passwords prevents the University from tracking which individuals make which changes to the database. Title 1, Texas Administrative Code, Section 202.75(3)(A), requires that all users of information resources be assigned unique identifiers and use their identifiers to gain access to applications.

  Furthermore, although the University asserts that this account is used only for certain activities, auditors observed one instance in which a database administrator performed a query using this account even though the query could have been run through the database administrator's own unique account.

- While there are two methods for database administrators to directly access the database—from the database server and from the network—users are only specifically identified when they access the database from the database server, not from the network. Not specifically identifying users prevents the University from tracking which individuals make which changes to the database.

- The database does not lock out accounts that have direct access to the database after multiple failed log-in attempts, and passwords for these accounts do not expire. Locking out accounts after failed log-in attempts is effective in preventing inappropriate access gained by guessing passwords, and requiring users to change passwords to their accounts decreases the likelihood that inappropriate users could guess valid passwords.

Recommendations

The University should:

- Ensure that the account with extensive database access is assigned to a specific individual, the password for this account is not shared, and the account is used only when a task requires the access that this account provides.
- Develop and implement a method for specifically identifying users who access the database through the network.
- Implement appropriate password controls for database user accounts that are similar to those described in the security policy for the financial system. These controls could include locking out user accounts after three failed log-in attempts and setting passwords to expire after 60 days.

Protecting the financial system. Financial information resources should be safeguarded in all areas of operation. The University should take steps to protect these resources from unauthorized access, modification, or destruction. The following items were identified in our review of the University's financial system operations:

- The University's server integrity files are stored on the same servers they are designed to protect. As a security measure, records of hash totals are created and used to detect and investigate changes in the file structure. This is a standard method for ensuring the integrity of data kept on servers. If a server were accessed by an unauthorized individual, the integrity files could be changed or destroyed, thereby eliminating the security measure the integrity files provide.
- The University is not using the built-in auditing capabilities of its financial system database. For example, the application does not record the activity of users who access the database directly. Direct database access is a privilege typically reserved for database administrators; therefore, it is important to monitor this activity to ensure the system's integrity.

Recommendations

The University should:

- Store master copies of the server integrity files on secure media, such as a write-once/read-only CD or DVD, to ensure that an attacker cannot access the files.
- Perform a risk assessment and cost-benefit analysis of activating the auditing capabilities in the financial system database. Based on the risk assessment, the University should activate the appropriate auditing functionality.

Status of recommendations made in fiscal year 2005 report.

In the November 2004 State Auditor's Office report on the University, 22 of the 28 recommendations related to information system security. Of these 22 recommendations, the University has fully implemented 11 and substantially implemented 6. Its implementation of three recommendations is ongoing, and the implementation of two recommendations is incomplete. (See the attachment for details.)

The University has controls in place to ensure that financial reporting is materially accurate; however, certain improvements can be made.

In addition to improving the financial system's security, other enhancements are necessary to make certain that financial report information is accurate. These enhancements are in areas such as emphasizing manual controls over system input; reviewing high-risk transactions; and ensuring the integrity, utility, and completeness of data. At the University, auditors found that:

- Controls do not prevent the miscoding of purchases in the University's financial system. Auditors tested a sample of purchase order line items for fiscal year 2005 and found a 6.45 percent rate of error in purchase coding. Most of these errors resulted in no financial misstatement. However, a more thorough review of 7,791 purchase order line items found that 106 were miscoded because staff incorrectly identified them as either capital assets or expensed purchases, which would affect financial reporting by misstating asset balances or expense amounts. These 106 items, totaling $743,980, could result in potentially misleading financial reports.

- Accounts Payable, as reported by the University at August 31, 2004, was understated by $12.1 million. This occurred because the University did not include in Accounts Payable $12.1 million in expenses paid in September 2004 for goods and services received prior to the end of the fiscal year. Generally accepted accounting principles require that expenses that are incurred during the fiscal year but not paid until the following fiscal year be recorded as outstanding liabilities in Accounts Payable.

- The University is not using its financial system application's preprogrammed auditing tools to their full potential. Currently, the University is logging only the creation of new vendor records. Logging and monitoring of high-risk entries and transactions, such as changes to vendor records, would help to ensure data integrity.

Recommendations

The University should:

- Provide effective training to individuals who make coding decisions and establish more effective review procedures to ensure that purchases are coded appropriately.

- Implement a procedure in its fiscal year-end closing process to ensure that expenses that are paid after the end of the fiscal year for goods and services received prior to the end of the fiscal year are included in Accounts Payable.

- Perform a risk assessment and cost-benefit analysis of activating the auditing capabilities of the financial system and configure the auditing tools based on the risks identified.

The University generally agrees with our recommendations, and its responses are included in the attachment to this letter.

We appreciate the University's cooperation during this audit. If you have any questions, please contact Dave Gerber, Audit Manager, or me at (512) 936-9500.

Sincerely,

John Keel, CPA
State Auditor

Attachment

cc: Chair and Members of the University of Houston System Board of Regents
Dr. G. Jay Gogue, University of Houston System Chancellor and University of Houston President

**Summary of
Objectives, Scope, and Methodology**

The audit objectives were to (1) determine whether controls within the University's financial system ensure that financial data and reports are accurate and (2) determine whether security controls within the University's financial system are adequate to protect critical data from unauthorized alteration, loss, or improper use.

The scope of our audit was limited to the University's financial system and the network on which the system resides. In following up on recommendations made in the 2004 report, our work was limited to recommendations applicable to the financial system and the network on which the system resides.

Our methodology consisted of reviewing the University's policies and procedures and those of the University of Houston System, conducting interviews with staff, and reviewing system settings and accounts. This audit was conducted in accordance with generally accepted government auditing standards.

In compliance with the Americans with Disabilities Act, this document may also be requested in alternative formats. To do so, contact our report request line at (512) 936-9880 (Voice), (512) 936-9400 (FAX), 1-800-RELAY-TX (TDD), or visit the Robert E. Johnson Building, 1501 North Congress Avenue, Suite 4.224, Austin, Texas 78701.

The State Auditor's Office is an equal opportunity employer and does not discriminate on the basis of race, color, religion, sex, national origin, age, or disability in employment or in the provision of services, programs, or activities.

To report waste, fraud, or abuse in state government call the SAO Hotline: 1-800-TX-AUDIT.

Attachment

Summary of Follow-Up Results

In November 2004, the State Auditor's Office released *An Audit Report on the Protection of Confidential Data and Critical Systems at the University of Houston* (SAO Report No. 05-010). The University of Houston (University) has made progress in implementing audit recommendations made in that report. However, additional action is needed for all audit recommendations to be completely implemented. Areas in which additional action is required include monitoring efforts, the University's wireless network, and the development of a comprehensive business continuity plan.

Table 1 provides an overview of the recommendations within the scope of our audit and the status of implementation as of October 14, 2005, as well as additional comments relating to the University's actions. See the text box for the definitions of implementation status.

Definitions of Implementation Status

- Fully Implemented: Successful development and use of a process, system, or policy to implement a prior recommendation
- Substantially Implemented: Successful development but inconsistent use of a process, system, or policy to implement a prior recommendation
- Ongoing: Successful development and consistent use of a process, system, or policy to implement a prior recommendation but implementation is not fully complete
- Incomplete: Ongoing development of a process, system, or policy to address a prior recommendation
- Not Implemented: Lack of a formal process, system, or policy to address a prior recommendation

Table 1

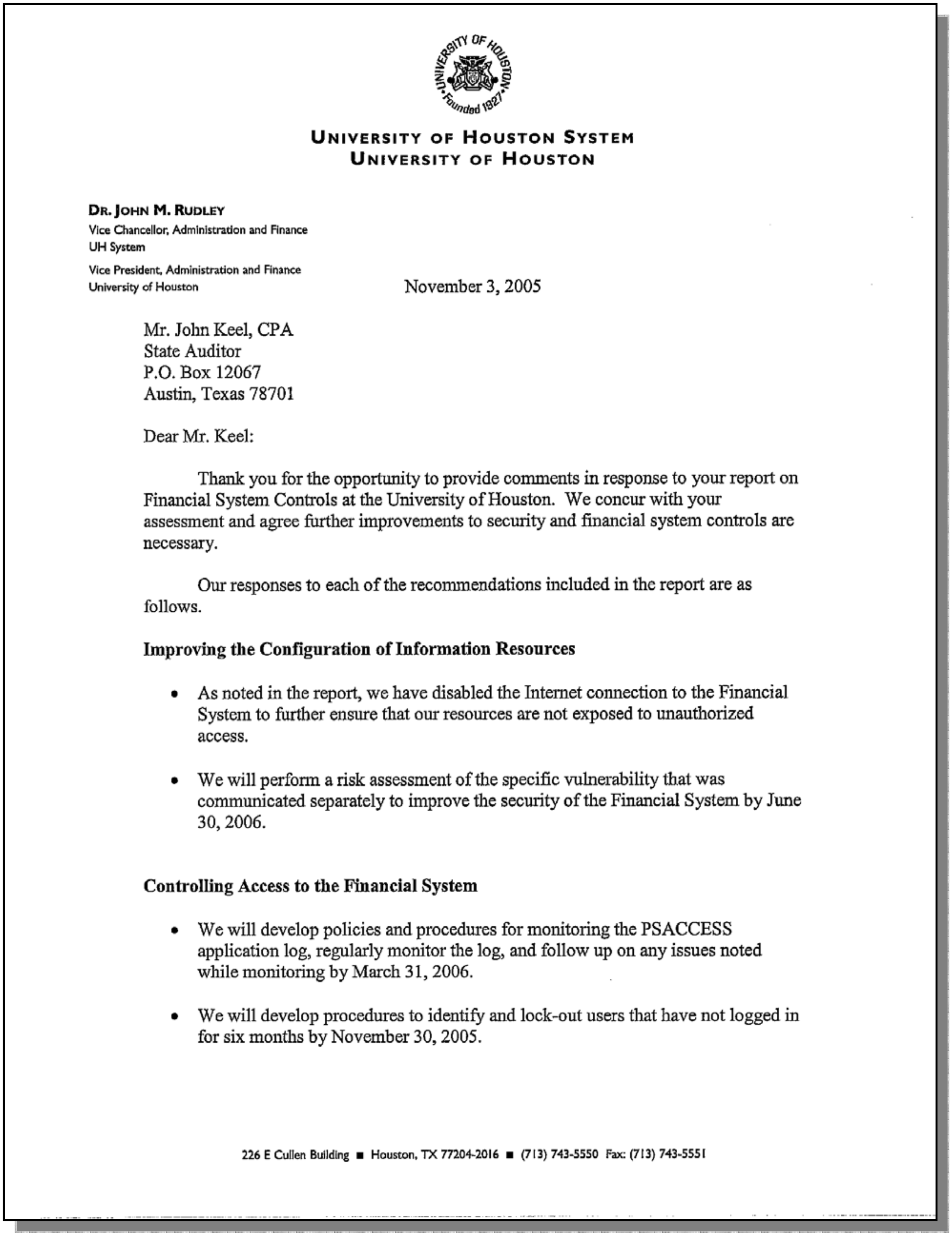
Status of the University's Implementation of Recommendations from SAO Report No. 05-010 - November 2004

Recommendation	Implementation Status	Auditor Comments
Ensure that database administrators do not have access to security functions and other applications. If implementing separation of duties is not practical, the University should implement regular supervisory reviews of security logs and changes to applications and databases made by database administrators.	Substantially Implemented	The University has implemented a procedure to limit database administrators' access to security functions. However, testing identified one instance in which a database administrator used an account with administrative security rights to the application.
Periodically review high-level user accounts to ensure that those accounts are still necessary.	Substantially Implemented	The University has reviewed and corrected internal procedures for the high-level access review process to ensure that high-level accounts are still necessary. However, testing identified high-level accounts that are still being shared by individuals who should have their own unique access rights.
Ensure that users have proper authorization documentation and approval to obtain high-level access.	Substantially Implemented	The University has reviewed and corrected internal procedures for the high-level access review process to ensure that high-level users always have proper authorization documentation. However, testing identified one user with access but for whom there was not proper authorization documentation.
Ensure that each user has his or her own unique user ID and password and that users do not share these IDs and passwords.	Substantially Implemented	The University has taken steps to ensure that each high-level user has his or her own unique user ID and password and that users do not share these IDs and passwords. However, auditors identified isolated instances of ID sharing.

Status of the University's Implementation of Recommendations from SAO Report No. 05-010 - November 2004		
Recommendation	**Implementation Status**	**Auditor Comments**
Monitor the access logs for high-level user accounts for specific security events to ensure that these accounts have not been compromised.	Incomplete	The University has taken steps to help ensure accountability over high-level user accounts. However, although access logs were being generated, they were not being reviewed.
Require all users of the wireless network to authenticate their identities using a user ID and password. This could be accomplished by redirecting all wireless access to an authentication page that requires the users to log in prior to allowing any access to the Internet or University network resources.	Ongoing	The University has implemented user ID and password wireless authentication on a limited scale. Wireless network users on the remainder of the campus were to begin using the new authentication process no later than October 31, 2005.
Require users to connect to the wireless network using the VPN or other applications that provide for encryption of data.	Fully Implemented	Users are required to connect to the University's critical systems identified within the scope of this audit using a secured method.
Rename all of its authorized wireless access points from the default SSID to a unique name.	Ongoing	Wireless access points are in limited use and are using the standard University SSID (Service Set Identifier). The remainder of the campus's access points were to begin using the standard University SSID no later than October 31, 2005.
Continue to install patches as needed.	Fully Implemented	The University is continuing to install patches as needed.
Use its scanning tools on a regular basis.	Fully Implemented	The University is scanning financial system resources on a regular basis to identify vulnerabilities.
Consider improving its monitoring of network traffic through the installation of additional intrusion-detection devices and increased monitoring of internal traffic.	Fully Implemented	The University improved its monitoring of network traffic by installing additional intrusion detection devices. The University is still using the same intrusion detection software, but it is considering expanding the use of this software or replacing it with another software program.
Develop, implement, and enforce procedures for disabling accounts for all systems when users no longer need access. This process should cover users who leave the University or change jobs within the University.	Substantially Implemented	The University has begun monitoring access. A list of terminated employees is reviewed and reconciled at least twice a month to determine whether access has been removed from terminated employees.
Review the list of stale user accounts and disable or remove all accounts for employees, students, and other users who do not use their accounts or who are no longer associated with the University.	Substantially Implemented	The University has updated its Finance Application Security Policy and has successfully implemented a process to identify and remove stale accounts. However, testing identified some inconsistencies. Although the University has shown improvement, there are still errors that can be corrected.
Revise its information security policies to require that, where possible, passwords be at least eight characters in length.	Fully Implemented	The University revised its *Information Security Manual* to require eight-character passwords that, when possible, include letters (upper- and lowercase), numbers, and special characters.
Ensure that, when possible, systems require the use of passwords that are at least eight characters in length and that are composed of letters, numbers, and special characters.	Ongoing	New password rules (minimum password length and character composition) will be implemented for the network by December 31, 2005.
Test its disaster recovery plan on an annual basis to ensure that the plan is adequate.	Fully Implemented	The University has tested its disaster recovery plan. The University also modified its procedures to recommend a systematic test of the disaster recovery plan every six months, with a minimum of one test per year.

Status of the University's Implementation of Recommendations from SAO Report No. 05-010 - November 2004		
Recommendation	**Implementation Status**	**Auditor Comments**
Develop a comprehensive business continuity plan that covers all business functions and incorporates all requirements of the Texas Administrative Code, including a business impact analysis.	Incomplete	The University has reviewed and modified its existing information technology disaster recovery plan. The development of a business continuity plan, including a business impact analysis, is currently in progress.
Ensure that all areas in which information resources are stored are adequately protected from environmental hazards and theft.	Fully Implemented	No further action was required of the University to address this recommendation. All items identified were corrected before the State Auditor's Office issued report number 05-010.
Update its security program.	Fully Implemented	The University has made updates to its information security program to incorporate the requirements of the Gramm-Leach-Bliley Act (GLBA); Title 1, Texas Administrative Code, Chapter 202; and other regulations.
Develop and implement an ongoing security awareness training program for all users. This program could be modeled after other programs in use at other institutions or programs developed by higher education information technology associations.	Fully Implemented	The University's human resources department administers the University's security awareness training program, which is presented to faculty on an annual basis. Eight more programs are also being designed. Additionally, in updating its information security program, the University included detailed information regarding its ongoing Information Security Awareness Training program.
Require all users to acknowledge their responsibility to comply with security requirements. It should also determine the method of acknowledgement and determine how often users must re-execute this acknowledgement.	Fully Implemented	All new users are required to acknowledge their responsibility to comply with the University's security requirements.
Require its information security officer to report to the appropriate level of management. At least annually, the information security officer also should report to the University's president on the status and effectiveness of information resources security controls.	Fully Implemented	The University has made the needed changes to its organizational structure. In addition, a status/effectiveness report for information resources security controls will be prepared and submitted annually to the University president.

Management's Response



UNIVERSITY OF HOUSTON SYSTEM
UNIVERSITY OF HOUSTON

DR. JOHN M. RUDLEY
Vice Chancellor, Administration and Finance
UH System
Vice President, Administration and Finance
University of Houston

November 3, 2005

Mr. John Keel, CPA
State Auditor
P.O. Box 12067
Austin, Texas 78701

Dear Mr. Keel:

Thank you for the opportunity to provide comments in response to your report on Financial System Controls at the University of Houston. We concur with your assessment and agree further improvements to security and financial system controls are necessary.

Our responses to each of the recommendations included in the report are as follows.

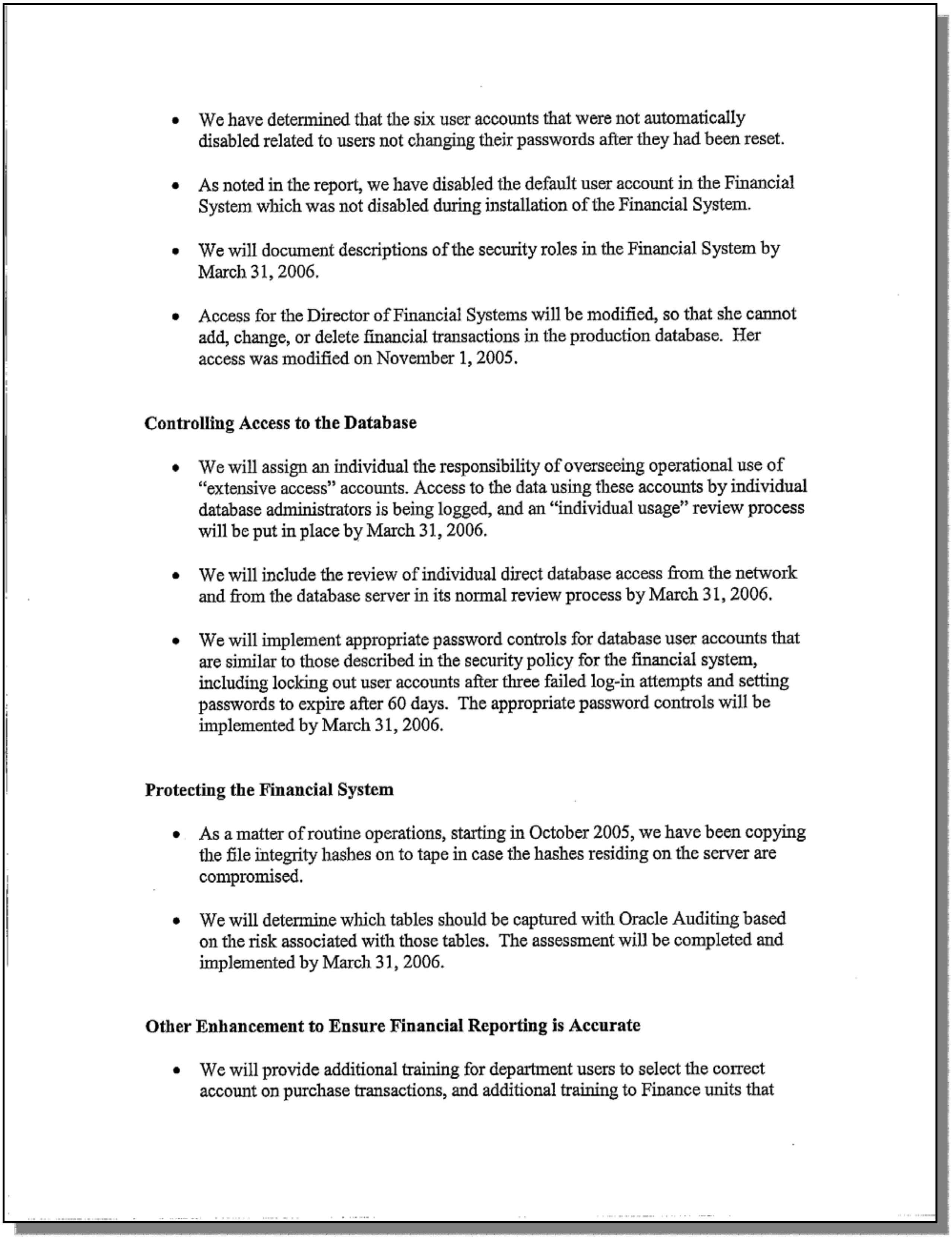
Improving the Configuration of Information Resources

- As noted in the report, we have disabled the Internet connection to the Financial System to further ensure that our resources are not exposed to unauthorized access.
- We will perform a risk assessment of the specific vulnerability that was communicated separately to improve the security of the Financial System by June 30, 2006.

Controlling Access to the Financial System

- We will develop policies and procedures for monitoring the PSACCESS application log, regularly monitor the log, and follow up on any issues noted while monitoring by March 31, 2006.
- We will develop procedures to identify and lock-out users that have not logged in for six months by November 30, 2005.

226 E Cullen Building ■ Houston, TX 77204-2016 ■ (713) 743-5550 Fax: (713) 743-5551



- We have determined that the six user accounts that were not automatically disabled related to users not changing their passwords after they had been reset.

- As noted in the report, we have disabled the default user account in the Financial System which was not disabled during installation of the Financial System.

- We will document descriptions of the security roles in the Financial System by March 31, 2006.

- Access for the Director of Financial Systems will be modified, so that she cannot add, change, or delete financial transactions in the production database. Her access was modified on November 1, 2005.

Controlling Access to the Database

- We will assign an individual the responsibility of overseeing operational use of "extensive access" accounts. Access to the data using these accounts by individual database administrators is being logged, and an "individual usage" review process will be put in place by March 31, 2006.

- We will include the review of individual direct database access from the network and from the database server in its normal review process by March 31, 2006.

- We will implement appropriate password controls for database user accounts that are similar to those described in the security policy for the financial system, including locking out user accounts after three failed log-in attempts and setting passwords to expire after 60 days. The appropriate password controls will be implemented by March 31, 2006.

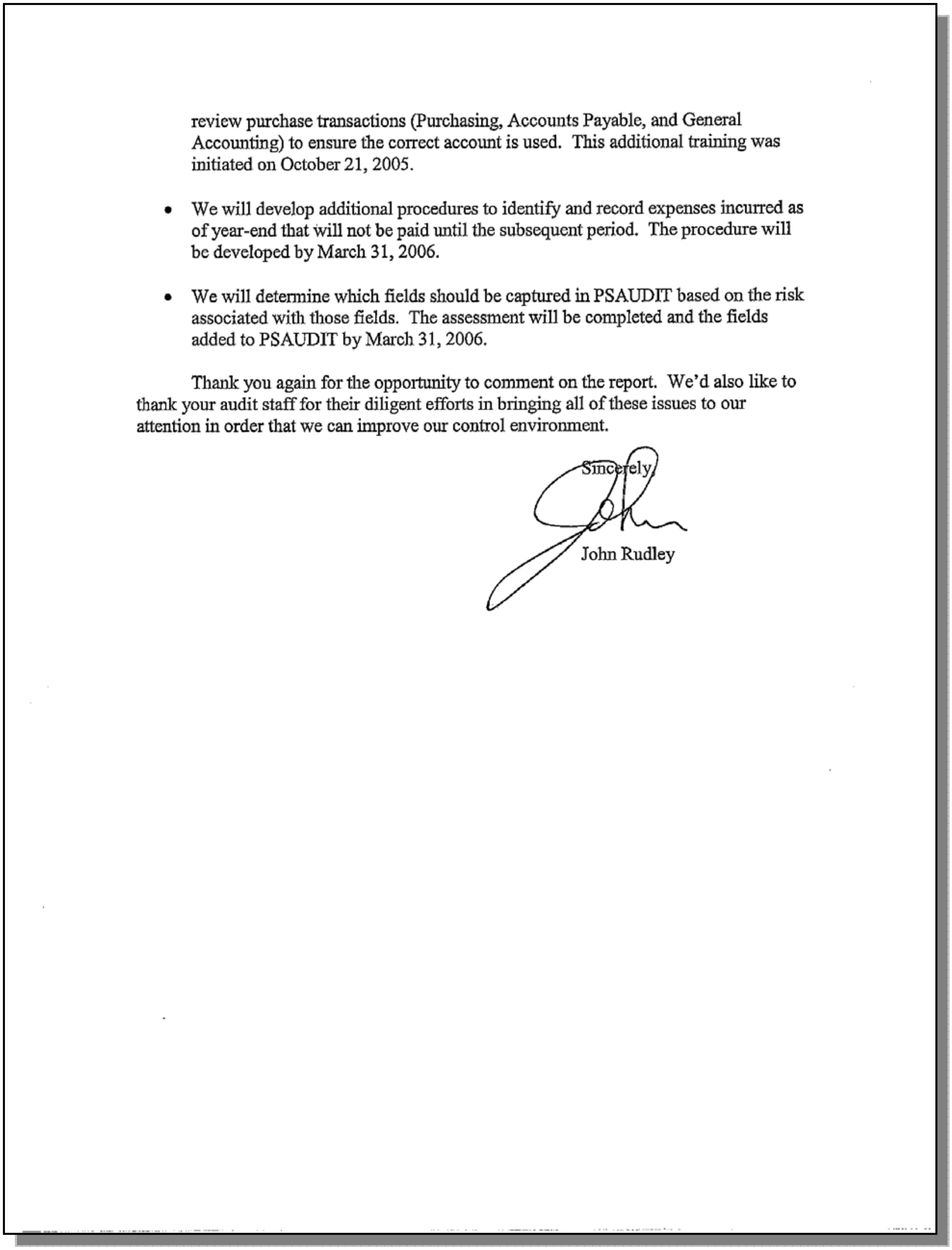
Protecting the Financial System

- As a matter of routine operations, starting in October 2005, we have been copying the file integrity hashes on to tape in case the hashes residing on the server are compromised.

- We will determine which tables should be captured with Oracle Auditing based on the risk associated with those tables. The assessment will be completed and implemented by March 31, 2006.

Other Enhancement to Ensure Financial Reporting is Accurate

- We will provide additional training for department users to select the correct account on purchase transactions, and additional training to Finance units that



review purchase transactions (Purchasing, Accounts Payable, and General Accounting) to ensure the correct account is used. This additional training was initiated on October 21, 2005.

- We will develop additional procedures to identify and record expenses incurred as of year-end that will not be paid until the subsequent period. The procedure will be developed by March 31, 2006.

- We will determine which fields should be captured in PSAUDIT based on the risk associated with those fields. The assessment will be completed and the fields added to PSAUDIT by March 31, 2006.

Thank you again for the opportunity to comment on the report. We'd also like to thank your audit staff for their diligent efforts in bringing all of these issues to our attention in order that we can improve our control environment.

Sincerely,

John Rudley