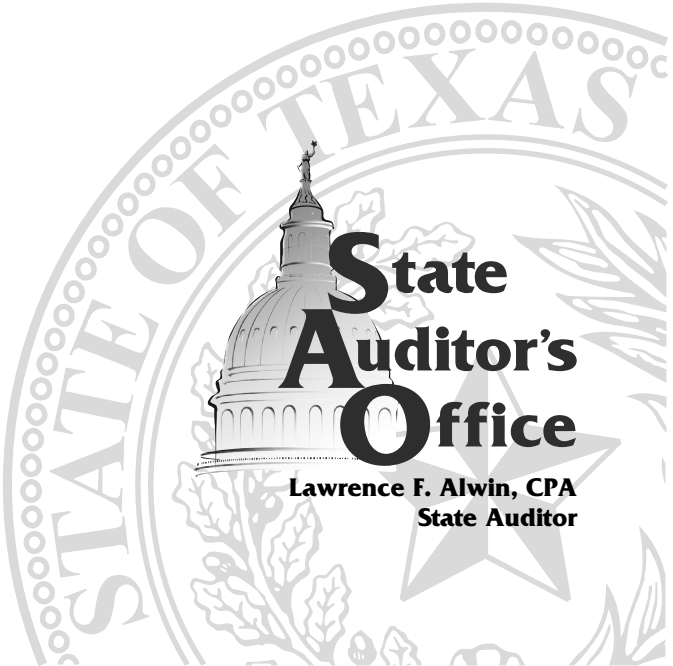
An Audit Report on

Cash Controls at the University of North Texas

August 2004

Report No. 04-049



State Auditor's Office

Lawrence F. Alwin, CPA
State Auditor

An Audit Report on

Cash Controls at the University of North Texas

SAO Report No. 04-049
August 2004

Overall Conclusion

Overall, the University of North Texas (University) has adequate controls over the receipt, safeguarding, and disbursement of cash. Furthermore, the University's controls over tuition, fee and housing revenues, petty cash reimbursements, student refunds and waivers, and deposits are adequate to ensure that transactions are accurately and completely recorded in accordance with state laws and regulations and University of North Texas System policies. We based our assessment on our evaluation of 11 University departments that handle 13 specific cash accounting functions.

Departments Evaluated

- Admissions
- Athletic Event Ticketing
- Coliseum
- Communications and Marketing
- Dining Services
- Financial Reporting (bank reconciliations)
- Housing
- Parking
- Purchasing and Payment Services (petty cash)
- Student Accounting
  - Student Refunds
  - Student Tuition and Fees
  - Student Waivers and Exemptions
- University Union

However, we found that the University's Athletic Department (Department) has several weaknesses in controls over the printing of and accounting for ticket sales that make the Department vulnerable to losses in revenues that it may not be able to detect. The University received approximately $257,000 in revenue from the sale of tickets to athletic events in fiscal year 2003.

We also found that the University has not yet adequately implemented security for its new financial accounting system, EIS FS, which it implemented in September 2003. There were weaknesses in EIS FS access controls, including inadequate standards for passwords and for user IDs and excessive privileges granted to users. These weaknesses could be exploited by an unauthorized user to create, modify, or delete financial data. However, we determined that the servers that house EIS FS were generally secure from internal and external threats such as those posed by hackers.

Summary of Information Technology Review

Our information technology work included a review of access and security controls for the EIS FS application, which is used to process all accounting transactions for the University. We also assessed controls for the Unix Operating System and Oracle Database that support the EIS FS application. Finally, we tested network security and wireless access to the servers on which EIS FS resides. We did not examine the University's student system or its architecture.

State Auditor's Office
Lawrence F. Alwin, CPA
State Auditor

This audit was conducted in accordance with Texas Government Code, Sections 321.0131 and 321.0132.

For more information regarding this report, please contact Ron Franke, Audit Manager, at (512) 936-9500.

Detailed Results

Chapter 1

The University Generally Has Adequate Cash Controls with the Exception of Two Departments

Overall, we found that the University of North Texas (University) has adequate controls over the receipt, safeguarding, and disbursement of cash. We evaluated 11 University departments that handle 13 specific cash accounting functions and found limited areas requiring improvement. We also found that, with minor exceptions, transactions relating to the cash functions tested were accurately and completely recorded in accordance with state laws and regulations and University of North Texas System policies.

However, controls in the University's Athletic Department (Department) over the receipt of cash and the system used to generate tickets are not adequate to (1) ensure that all cash receipts and related revenues are deposited and accounted for or (2) prevent or detect the manipulation of ticket sales. The Department received approximately $257,000 in revenues during fiscal year 2003 from the sale of event tickets.

In addition, the Payroll Department should improve the management of the payroll bank account.

Chapter 1-A

Weaknesses in the Athletic Department's Controls Create a Risk that Cash Receipts and Event Tickets Could Be Diverted or Misused

The Department is not taking adequate steps to ensure that it receives all revenue from ticket sales. We identified control weaknesses that create a risk that tickets could be diverted or misused.

The Department does not fully reconcile athletic event revenues to tickets printed and sold. The Department does not reconcile the total event revenue to tickets that are sold, returned, never issued, or given out on a complimentary basis. As a result, it cannot ensure that all revenue is collected and may not be able to detect the selling of tickets for personal gain.

Table 1: For the three events audited, the actual number of game-day tickets returned unsold was less than the number recorded in Ticketmaster.

Event	Ticketmaster Detail Report - Unsold Tickets	Ticket Count	Difference
Baylor	11,700	6,945	(4,755)
Houston	140	126	(14)
Indiana	80	68	(12)

The need for a full reconciliation was evident in our testing of three athletic events. We compared the number of unsold tickets in the ticketing system detail reports to the number of unsold tickets returned after the game. In each case, the number of returned tickets was less than the reported unsold tickets (see Table 1). We were unable to determine why the

number was less, but we were able to account for the deposit of all but $30 of the game day revenue for the three games. Our work was complicated by the fact that, for two of the events, the detail reports from the ticketing system did not match the summary reports.

The Department does not adequately control or monitor access to its ticketing system. Because Department employees share logins to the ticketing system, there is no record of which employees handle specific transactions. This is significant because the ticketing system allows employees to print a ticket but enter it into the system as "unsold," making it possible for the employees to sell tickets for personal gain without detection.

We also found that, of 12 active user IDs and passwords to the ticketing system, 3 were for student assistants who were no longer employed by the Department. The other nine users appear to have excessive privileges for ticketing operations, including the ability to change ticket prices, process ticket returns, and reprint tickets.

The Department does not use a mail log or receipt book to document payments it receives by mail. Because the Department does not document mail receipts (primarily checks and credit card orders) at the time the mail is opened, it cannot determine whether all receipts have been deposited and recorded to the University's accounts. It is also unlikely to detect the loss or theft of receipts, and it may inadvertently fail to comply with Texas Education Code, Section 51.0003(b), which requires that all collections be deposited within seven days after receipt.

Recommendations

The Department should:

- Perform complete and timely reconciliations to ensure that it has received and deposited all ticket revenue due. These reconciliations should be performed by individuals who are not involved in the processes of printing tickets or collecting receipts, and they should be reviewed by management.
- Require that employees log in individually to the ticketing system so that there is an adequate record of responsibility for ticketing transactions.
- Establish and implement system and manual controls to ensure that tickets cannot be entered into the ticketing system as unsold but actually be printed and sold for personal benefit.
- Ensure that access to the ticketing system is removed immediately upon employee termination.
- Restrict employees' access to the ticketing system according to the functions that individual employees perform.
- Document all payments received through the mail in a mail log or receipt book.

Management's Response

- *Management agrees with the recommendation. Complete event reconciliations for the 2004-05 season will be performed by the Assistant Athletic Director for Business Operations and/or the Athletics Business Office staff. The number of full-time staff in the ticket office, the overlap of events and seasons, and the additional responsibilities of the staff involved, are all factors that impact the timeliness of the reconciliations. However, it is the goal of the Athletics Department to have a preliminary reconciliation for each event completed in a timely manner. Final reconciliations will be completed after all accounts receivables (payroll deductions, Electronic Funds Transfers, corporate sponsorships) are received and processed in the ticketing system.*

- *Management agrees with the recommendation. Effective immediately, all staff responsible for assisting with the selling of tickets will be required to log in and out of the ticketing system individually with their own ID and password to create an adequate trail of ticketing transactions.*

- *Management agrees with the recommendation. Effective immediately, the Athletics Department will begin using a "2nd authorization" process before any tickets involved in a cash transaction are allowed to be unsold in the ticketing system. Any and all staff involved in a cash transaction that requires tickets to be processed as "unsold", will be required to receive an additional authorization from his/her supervisor before the transaction is completed. A log will be kept of all cash transactions that involve unsold tickets and this log will be reconciled to individual game reports and batch reports. In addition, the department's new access manager system will not allow the bearer of an "unsold" ticket to enter the stadium.*

- *Management agrees with the recommendation. All employees will immediately have their access deactivated upon termination. The names of any and all users will be archived for future reconciliation purposes. The access ID's for the three student-users referenced in report have been deactivated.*

- *Management agrees with the recommendation. The Athletics Department will begin a review of all users, their job functions, and their needs as it pertains to the ticketing system and the effective operation of the Athletics Department.*

- *Management agrees with the recommendation. The Ticket Office will begin using a mail log or receipt book to document all payments received through the mail.*

- *The Assistant Athletic Director for Business Operations will be responsible to ensure the timely implementation for each of the changes in procedures.*

Chapter 1-B

The University Has Not Investigated and Resolved Numerous Old Reconciling Items in Its Payroll Bank Account

While bank reconciliations for other University accounts were up to date and in good order, we found that the reconciliation for the payroll account contained reconciling

items dating back to 2001. Although the total net effect of these reconciling items as of August 31, 2003, was only $422.10, actual errors and fraud may go undetected when reconciling items are not resolved and cleared in a timely manner. While the reconciliation process would not necessarily identify payroll fraud of the type the University experienced in 2004 involving employees who should not have been on the payroll, it could identify counterfeit checks or checks with altered amounts.

Recommendation

The University Financial Reporting Office and Payroll Department should take timely action on the resolution of reconciling items in the payroll bank account.

Management's Response

The Assistant Director of Financial Reporting has already begun to assume a more proactive approach to clearing reconciling items.

Chapter 2

Security Controls for the University's Financial Systems Need Improvement

The University has not yet adequately implemented security for its new PeopleSoft financial application (EIS FS), which is used to process all accounting transactions for the University. The University implemented EIS FS in September 2003. We found weaknesses in EIS FS access controls, including inadequate user ID and password standards and excessive access granted to users and administrators. Access controls should also be improved for the operating system and database that support EIS FS (see text box).

Web-Enabled Systems Require Strong Application-Level Security

Users of EIS FS can access the system through the Internet, which is beneficial to the users. At the same time, making an application available through the Internet takes away the security that comes with limiting the number of computers that run the application. As a result, the importance of security controls at the application level—such as user IDs and passwords—is increased.

Source: *Security, Audit and Control Features for PeopleSoft: A Technical and Risk Management Reference Guide*

Results of our tests of network security and wireless access indicate that the servers that support EIS FS are generally secure from both internal and external threats. The University mitigated vulnerabilities identified during the course of our work.

Chapter 2-A

Weaknesses in Controls for EIS FS Increase the Risk of Unauthorized Access

Standards for user authentication (the method used to ensure that individuals accessing a system are authorized users) are not sufficient to prevent unauthorized access to EIS FS. In addition, some users and administrators have excessive access to EIS FS. As a result, there is a risk that an unauthorized user could create, modify, or delete the University's financial data.

Standards for user authentication. Faculty, staff, and students are granted enterprise user identifications (EUID), which are used for access to EIS FS accounting, online registration, and other systems. Weaknesses in the administration of EUIDs include the following:

- The University does not disable or delete EUIDs. This could potentially allow former staff, faculty members, and students unauthorized access to information resources, including EIS FS, for long periods of time.

- The University does not require users to change their EUID passwords and does not enforce minimum password length and complexity standards.

- There is no intruder lockout policy to protect against unauthorized access by someone who is attempting to access information resources by guessing passwords.

Access rights. At the time of our review, 48 percent of all active EIS FS user accounts had full authority rights within EIS FS, meaning that these users have the ability to create, modify, and delete EIS FS data without restriction.

The University does not have documented procedures for managing the process of creating users' roles to ensure privileges are appropriate and follow basic control concepts such as separation of duties. Also, the University has not fully implemented the EIS FS security features that define the functions users are allowed to perform. These features are included in EIS FS so that the University can build security around its business processes.

We also found that eight individuals share the PSAdmin account. If any of these individuals were to make inappropriate changes to EIS FS, it would not be possible to determine who was responsible. The PSAdmin account allows these individuals to go through EIS FS to access the database that supports EIS FS. (As discussed in Chapter 2-B, there are also user account issues for users with direct access to the database.) It is also used by the EIS FS application itself to post transactions to the database tables.

Warning banner. There is no warning banner when users log in to EIS FS. Section 202.8 of the Texas Administrative Code (TAC) requires that such banners inform users of state information resources that:

- Unauthorized use is prohibited.

- Usage may be subject to security testing and monitoring.

- Misuse is subject to criminal prosecution.

- There is no expectation of privacy except as otherwise provided by applicable privacy laws.

Recommendations

The University should:

- Disable EUIDs for staff and faculty upon termination, and disable student EUIDs after a predefined period of inactivity.

- Require users to change their passwords periodically, and ensure that passwords meet minimum length and complexity standards.

- Implement a log-in warning banner for EIS FS in compliance with TAC 202.8.

- Review EIS FS accounts to ensure that privileges granted to all users are warranted. Accounts should be set up to allow only the functions users need to perform their duties.

- Take advantage of the security controls PeopleSoft built into EIS FS.

- Formalize and document the process for obtaining management approval before creating user accounts.

Management's Response

General Statement: The University agrees with the recommendations and would also like to point out that most, if not all of them, would have eventually been implemented with the complete installation of the new EIS system. We are still trying to catch our breath.

- *Management agrees with the recommendation. The University's policy on EUIDs is that each assigned EUID will remain attached to a single individual for the life of the EIS system in order to perpetuate the individual's relationship with the university. The level of access to the system provided by that EUID, however, will be changed based upon the individual's status at the University or the Health Science Center. Human Resources is formulating a policy for staff and faculty access to HR self-service and Student Services is responsible for formulating the policy for retention of student self-service access in EIS Learning Solutions.*

  The current policy for EIS Financials is that only benefits-eligible staff members are given access when their job responsibilities determine that access is required, and that access is defined and limited by their roles. Upon their termination, all their roles are removed from the user account, the password is changed, and the account is locked.

  Because students will need access to the EIS long after they have left the University or HSC for such purposes as requesting a transcript or making contributions to the Alumni fund, accounts will not be fully disabled after some period of inactivity. However, students' access to such functions as course registration, financial aid, and advising will be disabled at the end of a twelve month period after the last term of enrollment. Students must then update their student records in order to determine eligibility for re-enrollment.

  Person responsible for implementation: Associate Vice President for Enrollment Management (Students,) Associate Vice President for Finance & Business Affairs (Financials)

  Time line for implementation: June 30, 2005

- *Management agrees with the recommendation. Procedures have been put into place that will require all users to change their passwords at least every 120 days, and passwords must meet minimum length and complexity standards. More*

information about these procedures can be found at http://www.unt.edu/benchmarks/archives/2004/august04/comp.htm. All passwords will be changed to strong ones by mid-December, 2004.

Person responsible for implementation: Executive Director for Information Technology and Academic Computing

Time line for implementation: All passwords will be changed to strong ones by mid-December, 2004.

- *Management agrees with the recommendation. The login warning banner will be implemented on the EIS portal login pages (my.unt.edu, myfs.unt.edu, and myls.unt.edu) by September 1, 2004.*

  Person responsible for implementation: Executive Director for Information Technology and Academic Computing

  Time line for implementation: September 1, 2004

- *Management agrees with the recommendation. All users have been reviewed and security access further defined. Currently, only 16 individual FS users have ALLPAGES. These users include the Family/Project Leads and the UNT & HSC Budget Offices (6 staff).*

  Person responsible for implementation: UNT Budget Director

  Time line for implementation: Completed

- *Management agrees with the recommendation. PeopleSoft requires the use of the PeopleSoft-delivered administrative account for support, installations, and patch processing. Eight individuals use this account in order to provide 24 x 7 support across multiple PeopleSoft environments. However these people have their own accounts with which they perform nearly all of the PeopleSoft administrative functions. It is our policy that the PSAdmins use their own accounts except where required by PeopleSoft.*

  This account is an integral part of the application messaging between/among the modules but it is quite limited in what Financial transactions it can post. No cash disbursements or check printing could be accomplished with this account.

  Should an inappropriate change be made by one of these eight individuals, we can look at the Oracle archive redo logs to determine when the change occurred, the IP network address, and program for the session where the user logged on.

  Person responsible for implementation: EIS Application Infrastructure Manager, Oracle Database Administrator

  Time line for implementation: February 1, 2005

- *Management agrees with the recommendation. UNT System is taking advantage of the PS delivered functionality, specifically by using Permission Lists, Roles and User Preferences (which are updated by department managers rather than by individual users as the name implies).*

It should be further noted that if an individual's user preference is not set to enable a certain functionality, the ACE's (Access Control Executives) cannot give additional security that would override the PPS management-defined User Preferences.

Person responsible for implementation: Access Control Security Service Lead,

Time line for implementation: Completed

- *Management agrees with the recommendation. A form has been developed to replace emails & memo requests. The form must be completed by individual department managers and security is updated by Access Control Executives (ACE's 2-UNT, 1-HSC).*

  FS Management has approved and the EIS Security team has implemented an automated process that creates user profiles (nightly) for all benefits-eligible employees in the EIS Financials Production environment. A base user role that was defined by EIS FS Management is attached to each user profile and the profiles are locked. FS department managers must authorize roles and permission lists for individual profiles for their department(s). The FS Management designated security specialists (ACE's) unlock the accounts and add appropriate functional roles based on the department managers' authorization.

  Person responsible for implementation: Associate Vice President for Finance & Business Affairs

  Time line for implementation: Completed

Chapter 2-B

Access Controls Should Be Improved for the Operating System and Database that Support EIS FS

Our limited reviews of access and security controls for the operating system and database that support EIS FS identified weaknesses in these areas.

Operating system. At least five individuals are sharing the root account for the operating system. The sharing of the root account could prevent the University from holding employees responsible for inappropriate actions. The root account provides "super-user" privileges to the operating system, which allow complete access to all files, directories, services, and commands. It does not appear that root passwords are changed on a regular basis.

Database. Although the University has enabled basic controls for direct access to the database that supports EIS FS, we found areas where these controls could be strengthened. (The database findings in Chapter 2-A apply to users who access the database by going through EIS FS. These findings relate to users with direct access.)

The system produces an audit log that details successful and failed log-ins. A database administrator monitors failed log-in attempts weekly. However, the logs of updates of critical data, software, and changes to security and access rules are not retained or reviewed. Additionally, there are 11 database user accounts with the

ability to insert, update, and delete records in EIS FS tables. Because no one keeps or reviews printouts of the updates, inappropriate changes might not be detected.

The University requires that users of the database change their passwords every 60 days. However, the database system does not enforce minimum password length and complexity standards. Furthermore, the two database administrators share the passwords for 13 system accounts. Insufficient password controls make the system vulnerable to unauthorized changes to financial data. TAC Section 202.7 requires entities to have authentication and password controls that comply with the entities' risk management decisions and industry best practices.

Recommendations

The University should:

- Provide each person who needs a root account for the operating system with his or her own account. Rather than having one root account that several users can access, the University should require these users to access root account privileges through their individual accounts.

- Require operating system users to change their passwords periodically, and ensure that passwords meet minimum length and complexity standards.

- Retain and review logs of updates to critical information, software, and changes to automated security or access rules.

- Ensure that database password controls comply with TAC 202.7, including minimum length and complexity standards.

Management's Response

- *Management agrees with the recommendation. Each system administrator with root access will be assigned a separate login account as recommended. The changes will be accomplished by the end of calendar year 2004.*

  Person responsible for implementation: EIS Technical Services Manager

  Time line for implementation: December 31, 2004

- *Management agrees with the recommendation. All account passwords will be changed at least every 120 days or upon system administrators' termination and will conform to password strength and aging standards that are described at http://www.unt.edu/benchmarks/archives/2004/august04/comp.htm. The password rule changes will be accomplished by the end of calendar year 2004.*

  Person responsible for implementation: EIS Technical Services Manager

  Time line for implementation: December 31, 2004

- *Management agrees with the recommendation. Oracle Auditing will be enabled and logs created to track when actions occur which represent changes to*

automated security and access rules including both Oracle security privilege use as well as changes to the Peoplesoft application security tables. In addition, Oracle Auditing will be enabled and logs created to track when updates to critical application files are made by users who have direct insert, delete, update to records in the EIS FS tables.

Changes to PeopleSoft Application software components are tightly controlled by STAT!, a Change/Version Control software product from Quest Software. The product tracks versions, and allows recovery of these changes; requires Managerial approval before changes can be migrated to the Production environments, and allows reporting of all changes. Application table changes are prepared by the programming staff, documented in the STAT! product, approved by management, and then performed by the PSAdmin staff. Oracle Auditing will be enabled and logs created to monitor when updates occur to schema objects containing the PeopleSoft application metadata so that changes made outside STAT! can be identified. Oracle Auditing will be enabled and logs created to identify when changes are made to application objects such as table structures, triggers, etc. that are not part of the PeopleSoft application metadata.

The Computing and Information Technology Center's Information Security team will periodically review the logs referenced above. The UNT System's Internal Audit office will review the procedures that are put into place for capturing and reviewing the logs.

Person responsible for implementation: Oracle Database Administrator (Oracle) UNT Information Security Coordinator (review of logs)

Time line for implementation: February 1, 2005

- *Management agrees with the recommendation. Oracle database administrators will institute strong password controls that comply with TAC 202.7, including minimum length and complexity standards.*

  Person responsible for implementation: Oracle Database Administrator

  Time line for implementation: December 31, 2004

Other Information

Objectives, Scope, and Methodology

Objectives

The project objectives were to determine the following:

- Whether the University of North Texas (University) has adequate controls for receiving, safeguarding, and disbursing cash.
- Whether the accounting and record-keeping of collections and of state revenues, receipts, and disbursements at the University are accurate and complete.
- Whether the University complied with state laws and regulations and with University and University of North Texas System policies related to cash management.

We also reviewed the University's safeguards over the information technology resources associated with the areas covered by these objectives.

Scope

The scope of this review included the accounting records and transactions for September 1, 2003, through January 31, 2004.

Methodology

To achieve these objectives, we:

- Interviewed University managers and staff.
- Reviewed University policies and procedures.
- Reviewed information systems used to collect and report financial information.
- Tested departmental cash receipts and bank reconciliations for the period of September 1, 2003, through January 31, 2004.
- Tested student waivers, refunds, exemptions, and petty cash accounts for the period of September 1, 2003, through January 31, 2004.

Project Information

We conducted fieldwork between April and July 2004. This review was conducted in accordance with standards applicable to performance audits contained in generally accepted government auditing standards.

The following members of the State Auditor's staff conducted the review:

- Agnes Barnes, CPA (Project Manager)
- Sharon Carney, CPA, MBA (Assistant Project Manager)
- Sharon Brantley
- David Dowden
- C. Y. Ihekwoaba, CPA
- Natasha Kelly, MBA
- Melissa Larson, CISA, CIA, CFE
- Jenay Oliphant
- Steve Sizemore, CIA, CISA, CGAP
- Mary Stauffer, CPA
- James Timberlake
- Dennis Ray Bushnell, CPA (Quality Control Reviewer)
- Ron Franke, MBA, CISA (Audit Manager)

Distribution Information

Legislative Audit Committee

The Honorable David Dewhurst, Lieutenant Governor, Joint Chair
The Honorable Tom Craddick, Speaker of the House, Joint Chair
The Honorable Steve Ogden, Senate Finance Committee
The Honorable Thomas "Tommy" Williams, Member, Texas Senate
The Honorable Talmadge Heflin, House Appropriations Committee
The Honorable Brian McCall, House Ways and Means Committee

Office of the Governor

The Honorable Rick Perry, Governor

The University of North Texas System

Mr. John Robert Ray, Chairman, Board of Regents
Mr. Charles Beatty, Member, Board of Regents
Ms. Marjorie B. Craft, Member, Board of Regents
Mr. Tom Lazo Sr., Member, Board of Regents
Mr. Robert A. Nickell, Member, Board of Regents
Mr. Burle Pettit, Member, Board of Regents
Mr. C. Dan Smith, Member, Board of Regents
Ms. Gayle W. Strange, Member, Board of Regents
Mr. Rice M. Tilley Jr., Member, Board of Regents
Mr. Lee Jackson, Chancellor

The University of North Texas

Dr. Norval F. Pohl, President