STATE OF NORTH CAROLINA

INFORMATION SYSTEMS AUDIT

CAMPUS PIPELINE APPLICATION

APPALACHIAN STATE UNIVERSITY

JUNE 2000

OFFICE OF THE STATE AUDITOR

RALPH CAMPBELL, JR.

STATE AUDITOR

INFORMATION SYSTEMS AUDIT

CAMPUS PIPELINE APPLICATION

APPALACHIAN STATE UNIVERSITY

JUNE 2000

STATE OF NORTH CAROLINA
Office of the State Auditor

Ralph Campbell, Jr.
State Auditor

2 S. Salisbury Street
20601 Mail Service Center
Raleigh, NC 27699-0601
Telephone: (919) 807-7500
Fax: (919) 807-7647
Internet http://www.osa.state.nc.us

AUDITOR'S TRANSMITTAL

The Honorable James B. Hunt, Jr., Governor
Members of the North Carolina General Assembly
Dr. Francis T. Borkowski, Chancellor

Ladies and Gentlemen:

We have completed our audit of the Campus Pipeline application at Appalachian State University (the University). This audit was conducted during the period from March 6, 2000 through April 14, 2000. We present this report for your consideration.

The primary objective of this audit was to determine if access controls over the Campus Pipeline application are effective. The scope of our audit included an assessment of the security architecture of the Campus Pipeline application and an assessment of the application and operating system configuration, specifically reviewing the access controls, data security, and network security over the application and the technical operating environment as implemented by the University.

This report contains an executive summary and audit results which detail the areas where improvements should be made to strengthen the access controls over the Campus Pipeline application and operating environment. During the course of our audit certain sensitive security related findings and recommendations were identified. Those sensitive issues were conveyed in detail to the University Information Technology Services personnel during the audit exit conference. Due to the sensitive nature of these issues, they will be reported more generically in this audit report. University Information Technology Services personnel have reviewed a draft copy of this report, and their written responses to each issue are included herein.

We wish to express our appreciation to the staff of the Appalachian State University Information Technology Services and Campus Pipeline, Inc. for the courtesy, cooperation and assistance provided to us during this audit.

North Carolina General Statues require the State Auditor to make audit reports available to the public. Copies of audit reports issued by the Office of the State Auditor may be obtained through one of the options listed in the back of this report.

Respectfully submitted,

Ralph Campbell, Jr.
State Auditor

cc: Dr. Harvey R. Durham, Provost and Vice Chancellor for Academic Affairs

Dr. Wilber Ward, Associate Vice Chancellor

TABLE OF CONTENTS

EXECUTIVE SUMMARY

We conducted an audit of the Campus Pipeline application at Appalachian State University (the University) between March 6, 2000 and April 14, 2000. The primary objective of this audit was to determine if access controls over the Campus Pipeline application are effective. Based on our objective, we report the following conclusions. They are organized into three categories: those related to the Campus Pipeline Application Software, those related to the administration of the Campus Pipeline application by the University, and those related to management issues.

CAMPUS PIPELINE APPLICATION

Following is a summarization of the findings we noted related to the Campus Pipeline application.

- The Campus Pipeline application software does not provide sufficient security features in the areas of user ID management, password management, and security violation and audit trail logging.
- The current Campus Pipeline application software, as configured by the University, allows access to sensitive and personal user profile information for students, faculty, and University employees anonymously using a standard web browser.
- The Campus Pipeline application tracks the application usage activities and web hand-offs of each user and transfers this information to Campus Pipeline, Inc. who uses the information in aggregate to assess the effectiveness of the application, evaluate the relevance of system features, and deliver targeted advertising to student and faculty users that is tailored to their interests. This tracking activity should be clearly disclosed to system users and should be further evaluated under the Family Educational Rights and Privacy Act (FERPA).

SYSTEM ADMINISTRATION

Following is a summarization of the findings we noted related to the system administration of the Campus Pipeline application.

- The University currently does not run the Campus Pipeline application or the Web for Students application in accordance with the network and hardware architecture recommended by the application vendors.
- We found inappropriate user access to numerous files on the UNIX server that hosts the Campus Pipeline application.
- The UNIX Systems Administrator has not been reviewing one of the audit logs kept by the UNIX operating system.

- We noted that a number of unnecessary services are running on the UNIX server that hosts the Campus Pipeline application. In addition, we noted that one system configuration setting allows all users of the system to perform activities that should be limited to the system administrator.
- We found that the current configuration of the UNIX server that hosts the Campus Pipeline application does not require that the operating system users periodically change their passwords.
- We noted that multiple system users share the administrator account on the UNIX operating System that hosts the Campus Pipeline application.
- We noted two user accounts that had inappropriate access to the UNIX operating system.
- The University currently is not applying University policy to notify the System Administrator of Campus Pipeline application and operating system users (students and faculty) who have separated from the University so that their logon IDs may be disabled.
- Virus protection software is not being used on the UNIX server that hosts the Campus Pipeline application.

MANAGEMENT CONTROLS

Following is the finding we noted related to the Management Controls.

- ASU does not have security policy and operating guidelines that govern the security of all University application systems.

SUMMARY

The overall control environment over the Campus Pipeline application running at Appalachian State University requires improvement for the application to be considered a well-controlled mission critical application. It should be noted that both Appalachian State University IT Services personnel and Campus Pipeline, Inc. have been very receptive to our suggestions during the audit. University IT Services personnel voluntarily addressed some findings we noted related to system administration while we were on site. Campus Pipeline, Inc. has made plans to quickly address the findings mentioned that relate to the application software.

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

Under the North Carolina General Statutes chapter 147-64, the State Auditor is responsible for examining and evaluating the adequacy of operating and administrative procedures and practices, systems of accounting, and other elements of State agencies. This audit was conducted at the request of the management of Appalachian State University. The objective of our audit was to determine if access controls over the Campus Pipeline application are effective. The scope of our audit is limited to the Campus Pipeline application and operating environment at Appalachian State University.

To accomplish our audit objective we reviewed the following.

- The application security architecture of the Campus Pipeline application, a vendor supplied software product, to ensure that the application offers effective data security controls.
- UNIX configuration and security for the UNIX server on which the Campus Pipeline application processes to ensure that the operating system server is configured in a manner to effectively secure the application and its data.
- Network Security over the immediate network to which the application server is attached to ensure that the network is configured in a manner to effectively secure data passing across the network to interfacing systems.
- Handling of student information by the Campus Pipeline application.

BACKGROUND INFORMATION

The management at Appalachian State University requested an audit of the Campus Pipeline application running at the University's data center to assess the information technology access controls over the application. The Campus Pipeline application is in production as a pilot application at Appalachian State University, and installation is planned at several other University of North Carolina campuses. This audit is intended to identify control weaknesses in the application and its administration so that they may be addressed prior to deployment of the application at the other Universities.

Campus Pipeline is a "portal" application that processes on a University web server and is accessible through the World Wide Web using a web browser. It is intended to be the means by which all University students and staff access most pertinent University information. It provides access to student account information, information on campus activities, classes, resources, libraries, schedules, etc. by interfacing with legacy University applications.

This "portal" technology is growing in popularity in a wide variety of organizations that have the goal of providing a simple, web-based user interface to provide access to various services and applications to a target population. The University of North Carolina system has plans to roll out the Campus Pipeline portal application at 5 universities and may eventually roll it out to 12 of the universities. Therefore, the work done on this project will benefit the installation of the application in each of the universities.

"Portal" technology offers the potential to tremendously improve service delivery by providing the ability for users to access centralized applications without having to install client software on their remote computers. The software used for a "portal" application is a standard web browser that exists on most computers connected to the World Wide Web. This application architecture provides greater accessibility to central applications than ever before possible at substantially lower costs.

While "portal" technology provides better service delivery at lower costs, it also may open up an organization's network to risks since the technology provides access to application systems through the World Wide Web. It is essential that this technology be implemented in a controlled fashion to reduce the associated risks and ensure the application, associated data, and telecommunications networks are used only by authorized personnel.

AUDIT RESULTS AND AUDITEE RESPONSES

The following audit findings identify the areas in the Campus Pipeline Application environment needing improvements.

CAMPUS PIPELINE APPLICATION

The following findings are associated with the Campus Pipeline application software, a packaged product provided by Campus Pipeline, Inc.

1. SECURITY FUNCTIONALITY

   The Campus Pipeline application does not provide the following basic security features:

   - Ability to set a minimum password length and password composition rules.
   - Ability to set Password expiration/change requirements.
   - Ability to lock logon IDs after an excessive number of failed login attempts has occurred.
   - Ability to suspend logon IDs after long periods of inactivity.

   We understand that these features will be available in the next release of Campus Pipeline.

   Because of the lack of these basic security features, the Campus Pipeline application is vulnerable to the following problems:

   - Hackers may be able to more easily guess passwords because users are not forced to use passwords that meet minimum requirements.
   - Hackers may be able to more easily steal passwords because of the lack of expiration/change requirements.
   - Hackers will have more potential accounts to attack because old accounts have not been locked due to inactivity.
   - Hackers will be able to use a "Cracker" program that repeatedly tries passwords for a given user name since an account is not locked after an excessive number of failed login attempts.

   If an unauthorized user gains access to the Campus Pipeline application, (s)he has the ability to drop or add courses for the authorized user, change schedules, or access transcript information (including grades and courses taken) and declared major information.

   Recommendation: The University should work with Campus Pipeline, Inc. to enhance the software to include these basic security features. Once the changes are made to the

application software, the University should be sure they are implemented on the production server running the application at the University.

Auditee Response: Campus Pipeline has implemented the following features for the next release of the Campus Pipeline product (codename "Orion"): the ability to set the minimum password length and composition rules, the ability to set password expiration and force a change of password, the ability to lock logon IDs after an excessive number of failed login attempts, and the ability to lock logon IDs after long periods of inactivity. This release is scheduled for general availability in July. Our plans are to implement this release immediately in order to take advantage of these features.

2. ACCESS TO SENSITIVE INFORMATION

The manner in which the Campus Pipeline application (as configured by the University) stores user information allowed us to access sensitive and personal user profile information for students, faculty, and University employees anonymously using a standard web browser.

The nature of this sensitive and personal information could allow an unauthorized user to more easily guess an authorized user's user name and password. Once the password has been compromised it would then be possible for the unauthorized user to access the system for malicious purposes. They could drop courses, add courses, access the student's academic records/ transcripts, and send emails as if they were the authorized student user. In addition, they could potentially use the personal user information to exploit the authorized user in a variety of ways.

Recommendation: The University should work with Campus Pipeline, Inc. to store the sensitive and personal information in the user profile in a secure manner that limits the access to only those authorized users who need access to this information to do their jobs. Once the changes are made to the configuration and if necessary to the application software, the University should be sure they are implemented on the production server running the application at the University.

Auditee Response: Campus Pipeline has modified the default configuration of the shipping product, Campus Pipeline 2.1.1, to disallow all unauthenticated access to information which may be sensitive and personal. Since Appalachian State is currently on this version of software, this access issue has been resolved.

3. SECURITY VIOLATION REPORTING AND AUDIT TRAILS

The Campus Pipeline application currently does not offer security violation logs or readily accessible audit trails to track user access to the system.

Security violation reports are detective controls used to identify potentially unauthorized access attempts and to detect suspicious usage activity such as access during non-business hours or access patterns that may indicate impropriety. Without these reports, it is much more difficult to identify and take action on suspicious login or usage activities.

Recommendation: The University should work with Campus Pipeline, Inc to build security violation reporting and audit trail features into the application code. Once the changes are made to the application software, the University should be sure they are implemented on the production server running the application at the University.

Auditee Response: For the release after "Orion" of the Campus Pipeline product (codename "Aquarius"), Campus Pipeline will implement the ability to send a security violation report to administrators for access patterns that may indicate impropriety and an audit trail service which provides the security administrator a summary of access patterns in the Campus Pipeline product. As we understand it, this release is slated for Fall 2000.

4. INFORMATION PRIVACY

The Campus Pipeline application tracks the application usage activities and web hand-offs of each user and transfers this information to Campus Pipeline, Inc. who uses the information in aggregate to assess the effectiveness of the Campus Pipeline application, to evaluate the relevance of system features, and to deliver targeted advertising to student and faculty users that is tailored to their interests.

The Buckley Amendment also called the Family Educational Rights and Privacy Act (FERPA) outlines rules regarding the protection of student information and educational records. One section of the FERPA legislation defines "education records" to include "those records, files, documents, and other material which contain information directly related to a student."

Recommendation: The University should review whether tracking the system usage and web browsing activities of students is adequately disclosed to users and whether it is a violation of this Act. At a minimum we believe that Campus Pipeline should disclose to all users that their activities within the application will be tracked for the purposes of assessing the effectiveness of the Campus Pipeline system, evaluating the relevance of system features, and targeting users with advertising. Students should be made aware of the disclosure statement so they understand how this information is being used.

Auditee Response: Campus Pipeline's privacy policy currently explains to users that the Campus Pipeline system tracks usage patterns in the aggregate to assess system effectiveness, evaluate the relevance of system features, and to enhance our services and offerings. In the version of the privacy policy that will appear in its next product release (codename "Orion"), Campus Pipeline will state expressly that usage patterns may be utilized to select or place advertising to be displayed to system users.

Campus Pipeline will provide to the University a copy of a legal memorandum prepared by a nationally recognized law firm on the question of whether tracking system usage would be construed as a violation of the Family Educational Rights and Privacy Act (FERPA).

The University will review this information and take appropriate actions as necessary to make sure we are in compliance and users are informed.

SYSTEM ADMINISTRATION

The following findings are associated with the system administration of the Campus Pipeline application. Many of the findings focus on the UNIX server that hosts the Campus Pipeline application. Any time UNIX is mentioned in this section, we are referring to the UNIX server that hosts the Campus Pipeline application.

5. APPLICATION ARCHITECTURE

Neither the Campus Pipeline application nor the Web for Students application are installed in accordance with the network and hardware architecture recommended by the application vendors.

Not having the Campus Pipeline application and Web for Students application configured in accordance with the recommendations from the application vendor could increase the vulnerability of the application, its data, and other applications on the University network.

Recommendation: The University should reconfigure the Campus Pipeline and Web for Students applications in accordance with the network and hardware architecture recommended by the application vendors.

Auditee Response: An internet firewall from Lucent Technology is now on site and in the process of installation. The entire CP application including the Web For, Tserver, and CP products are behind this firewall.

6. FILE ACCESS

We found numerous files on the UNIX operating system that had inappropriate access rights.

Access to all files on the UNIX operating system should be granted in accordance with users job functions.

Recommendation: The UNIX system administrator should change all UNIX file permissions to grant file access in accordance with users job functions. The specific file

permissions in question have been communicated to the appropriate IT Services personnel.

Auditee Response: We will immediately remove all world writable settings as needed.

7. SECURITY LOGS

The UNIX Systems Administrator has not been reviewing one of the audit logs kept by the UNIX operating system. This log is used to identify missing log information or unusual activities that may indicate unauthorized system usage.

Unauthorized activities could occur without detection on the UNIX server.

Recommendation: The UNIX System Administrator should review all audit logs to identify missing log information or unusual activities and take appropriate follow-up action.

Auditee Response: This shortcoming has been duly noted and will be instituted as a part of our job. We periodically monitored the "last" log which would trigger off suspicious entries made by users based on the IP address of the accessing node.

8. UNIX CONFIGURATION

We noted that a number of unnecessary services are running on the UNIX server. In addition, we noted that one system configuration setting allows all users of the system to perform activities that should be limited to the system administrator.

These services and configuration settings increase the vulnerability of the operating system and the hosted application to malicious attack.

Recommendation: The University should disable all unnecessary services on the UNIX server and configure the operating system to limit system administration activities to only the system administrator.

Auditee Response: We have eliminated all unnecessary services which are not needed for the Campus Pipeline application.

9. PASSWORD AGING

We found that the current configuration of the UNIX server does not require that the operating system users periodically change their passwords.

If a password is compromised, both the authorized user and the unauthorized user would have access to the user account indefinitely.

Recommendation: The University should configure the UNIX server to require operating system users to periodically change their passwords in accordance with the University Information Security Policy.

Auditee Response: We agree with the finding and will implement the change.

10. ADMINISTRATOR ACCOUNT

We noted that multiple system users share the administrator account on the UNIX operating system.

Allowing multiple users to use the same Campus Pipeline administrator account decreases individual accountability. Unauthorized activities could take place using this account and the University would not be able to identify which of the users was responsible for the unauthorized activities.

Recommendation: The University should create unique accounts for each user with system administration responsibilities and not allow system administrators or users to share accounts.

Auditee Response: We agree with the finding and have implemented the change.

11. USER ACCESS RIGHTS

We noted two user accounts that had inappropriate access to the UNIX operating system.

The access granted to these two user accounts increases the vulnerability of the UNIX operating system and the Campus Pipeline application to activities that could corrupt the application or affect normal operation.

Recommendation: The University should take action to eliminate the inappropriate access to the UNIX operating system. Detailed recommendations have been communicated to the appropriate University IT Services personnel.

Auditee Response: We agree with the finding and have implemented the change.

12. ACCOUNT MANAGEMENT

The University currently is not applying University policy to notify the System Administrator of Campus Pipeline application and operating system users (students, faculty, and University employees) who have separated from the University so that their logon IDs may be disabled.

Terminated employees or departing students could use their logon IDs and system resources in a malicious manner. In addition a third party could use the logon ID of a terminated employee or student without detection since the authorized user is no longer employed or enrolled and using the logon ID.

Recommendation: The University should follow established policy and procedures to identify terminated or separated personnel and pass the information onto system administrators who should take immediate action to disable the Campus Pipeline application and operating system logon IDs.

Auditee Response: A system is currently in place, which identifies the students who are new, reactivated, and who have left. The processing has not currently been extended to Campus Pipeline, but will be incorporated during this summer. We do have an alternative way to identify the students who are inactivated, deleted, and active. We are still refining the way faculty and staff are handled by using the Payroll system. Our internal auditors are helping us with this process.

13. VIRUS PROTECTION

Virus protection software is not used on the UNIX server.

Without up-to-date virus protection software running on the host computer, a virus could infect the computer resulting in adverse conditions that could include data and file corruption, disablement of application processing, or disablement of processing on other computers connected to the Campus Pipeline server through a trusted network connection.

Recommendation: The University should purchase, install, and maintain virus protection software on the host UNIX server and on any other computers connected to the Internet.

Auditee Response: While we agree that a server based filtering software to control virus proliferation would be optimum, users are currently responsible for that protection with client workstation software. The University has a site license with McAfee for all campus owned equipment. Many of the computers purchased for personal use come with Norton. We will investigate server based software options for virus protection and then make a determination of the best course of action.

MANAGEMENT CONTROLS

The following finding is associated with management controls over the Information Technology environment at Appalachian State University.

14. SECURITY POLICY

ASU does not have an information system security policy and operating guidelines that govern the security of all university application systems.

Until recent years, all ASU application systems ran on a central DEC VAX mainframe computer. ASU has limited policies that define some security standards over DEC VAX application systems. Growth of applications outside the DEC VAX platform standard has left the University without information security policy and operating guidelines that address all ASU application systems.

The lack of an information security policy and operating guidelines leads to inconsistent and often times inadequate implementation of security controls over University applications.

Recommendation: The University should develop information security policy and operating guidelines that define the security standards for ASU application systems. The policy should state the University's position on securing University applications, operating systems, and networks. At a minimum the guidelines should address the following:

- Unique identification of all application system users.
- Authorized Logon ID and password requirements for access to University applications.
- Policy against sharing Logon IDs.
- Minimum password length and password composition.
- Password expiration/change requirements.
- Account locking due to excessive number of failed login attempts.
- Revocation of logon IDs immediately at termination.
- Suspending logon IDs after long periods of inactivity.

Auditee Response: The University will develop and implement a security policy.

DISTRIBUTION OF AUDIT REPORT

In accordance with G.S. § 147-64.5 and G.S. § 147-64.6(c)(14), copies of this report have been distributed to the public officials listed below. Additional copies are provided to other legislators, state officials, the press, and the general public upon request.

EXECUTIVE BRANCH

The Honorable James B. Hunt, Jr.	Governor of North Carolina
The Honorable Dennis A. Wicker	Lieutenant Governor of North Carolina
The Honorable Harlan E. Boyles	State Treasurer
The Honorable Michael F. Easley	Attorney General
Mr. Marvin K. Dorman, Jr.	State Budget Officer
Mr. Edward Renfrow	State Controller

LEGISLATIVE BRANCH

Appointees to the Joint Legislative Commission on Governmental Operations

Senator Marc Basnight, Co-Chairman	Representative James B. Black, Co-Chairman
Senator Frank W. Ballance, Jr.	Representative Martha B. Alexander
Senator Patrick J. Ballantine	Representative E. Nelson Cole
Senator Roy A. Cooper, III	Representative James W. Crawford, Jr.
Senator James Forrester	Representative W. Pete Cunningham
Senator Wilbur P. Gulley	Representative Ruth M. Easterling
Senator David W. Hoyle	Representative Joe Hackney
Senator Howard N. Lee	Representative Thomas C. Hardaway
Senator Fountain Odom	Representative Martin L. Nesbitt
Senator Beverly M. Perdue	Representative Edd Nye
Senator Aaron W. Plyler	Representative William C. Owens, Jr.
Senator Anthony E. Rand	Representative Liston B. Ramsey
Senator Robert G. Shaw	Representative E. David Redwine
Senator Ed N. Warren	Representative Stephen W. Wood
Senator Allen H. Wellons	Representative Thomas E. Wright

Other Legislative Officials

Senator Eric Reeves	Chairman for the Committee on Information Technology
Representative Phillip A. Baddour, Jr.	Majority Leader of the N.C. House of Representatives
Representative N. Leo Daughtry	Minority Leader of the N.C. House of Representatives
Representative Joe P. Tolson	Co-Chairman for the Committee on Technology
Representative Drew P. Saunders	Co-Chairman for the Committee on Technology
Mr. James D. Johnson	Director, Fiscal Research Division

June 16, 2000

ORDERING INFORMATION

Copies of this report may be obtained by contacting the:

Office of the State Auditor
State of North Carolina
2 South Salisbury Street
20601 Mail Service Center
Raleigh, North Carolina 27699-0601

Telephone: 919/807-7500

Facsimile: 919/807-7647

E-Mail: reports@ncauditor.net

A complete listing of other reports issued by the Office of the North Carolina State Auditor is available for viewing and ordering on our Internet Home Page. To access our information simply enter our URL into the appropriate field in your browser: **http://www.osa.state.nc.us**