Claire McCaskill
Missouri State Auditor

May 2006

HIGHER EDUCATION

FAMOUS System Data Confidentiality and Security

Report no. 2006-30

auditor.mo.gov

Claire McCaskill
Missouri State Auditor

YELLOW SHEET

Confidential Student Data is Vulnerable to Unauthorized Disclosure and Use This audit reviewed the security controls and policies and procedures used by Department of Higher Education (DHE) and Information Technology Services Division (ITSD) officials to ensure the confidentiality, integrity and availability of student records maintained in the Financial Assistance for Missouri Undergraduate Students (FAMOUS) system.

No assessment of operating risks	DHE and ITSD officials had not conducted an assessment of the risks of operating the FAMOUS system. Accepted standards state a risk assessment helps identify potential threats and vulnerabilities, the resulting impact, and the appropriate controls needed to reduce the impact and achieve and maintain an acceptable level of risk. (See page 4)
Missing security features leave student data and system at risk	DHE and ITSD officials implemented the FAMOUS system without many commonly accepted security features. The basic security features in FAMOUS consist of access rights granted to user IDs and the use of passwords to authenticate IDs. However, common security features (such as a requirement to change passwords on a scheduled basis, the capability for users to change passwords themselves, and a system-required minimum password length) required by accepted standards are not yet available to help safeguard FAMOUS. An ITSD official said DHE and ITSD staff are working on implementing additional software to manage system security which should be in place by the start of the 2006/2007 school year. (See page 5)
Documented policies needed to ensure security of operations	DHE has developed procedures for operating the FAMOUS system but has not yet formally documented essential procedures and associated policies for these operational security controls. Formalizing operational practices and procedures with sufficient detail helps to eliminate security lapses and oversights, gives new personnel sufficiently detailed instructions, and provides a quality assurance function to help ensure operations will be performed correctly and efficiently, according to accepted standards. (See page 6)

All reports are available on our website: www.auditor.mo.gov

Contents

State Auditor's Letter 2

Confidential Student Data is Vulnerable to Unauthorized Disclosure and Use 3

Background 3
Scope and Methodology 4
Operating Risks Are Not Assessed 4
Security Features Leave Student Data and System at Risk 5
Documented Policies are Necessary to Ensure Security of Operations 6
Conclusions 8
Recommendations 9
Agency Comments 9

Abbreviations

DHE	Department of Higher Education
FAMOUS	Financial Assistance for Missouri Undergraduate Students
FERPA	Family Educational Rights and Privacy Act
ITSD	Information Technology Services Division
User ID	User Identification

CLAIRE McCASKILL
Missouri State Auditor

Honorable Matt Blunt, Governor
and
Dr. Greg Fitch, Commissioner
Department of Higher Education
Jefferson City, MO 65102

The Department of Higher Education (DHE) provides financial assistance for undergraduate college students through several grant and scholarship programs. DHE administers these financial assistance programs using the Financial Assistance for Missouri Undergraduate Students (FAMOUS) system. The Office of Administration, Information Technology Services Division (ITSD) is responsible for providing technical assistance to support DHE's information systems. The audit's objective was to determine whether DHE and ITSD officials have implemented security controls and developed policies and procedures to ensure the confidentiality, integrity and availability of student records and the FAMOUS system.

We found DHE and ITSD had not taken all the measures necessary to fully protect the confidentiality of student records maintained in FAMOUS. The department had not performed a current risk assessment to identify security controls required to protect FAMOUS from potential threats and vulnerabilities. While we identified some security features within the system, we determined critical security features were still missing. We also identified instances where critical policies and procedures had not been documented.

Our audit was conducted in accordance with applicable standards contained in *Government Auditing Standards*, issued by the Comptroller General of the United States, and included such procedures as we considered necessary in the circumstances. This report was prepared under the direction of John Blattel. Key contributors to this report were Jeff Thelen and Lori Melton.

Claire McCaskill
State Auditor

Confidential Student Data is Vulnerable to Unauthorized Disclosure and Use

Confidential data stored on the Financial Assistance for Missouri Undergraduate Students (FAMOUS) system is vulnerable to unauthorized disclosure, modification, use or destruction. This situation has occurred because the Department of Higher Education (DHE) had not completed a current risk assessment to identify possible threats and the likelihood of occurrence, implemented appropriate security features to mitigate risks and documented key security policies and procedures. Collectively, these weaknesses impair DHE's ability to ensure the confidentiality, integrity and availability of data and to ensure compliance with the Family Education Rights and Privacy Act (FERPA).

Background

DHE is responsible for determining eligibility and awarding financial assistance through various grants and scholarships to undergraduate college students attending participating post-secondary institutions in the state. Each of these financial assistance programs has different eligibility requirements. For the 2005/2006 school year, DHE administered the following six financial assistance programs using the FAMOUS system:

- Advantage Missouri Program
- Charles Gallagher Student Financial Assistance Program
- Marguerite Ross Barnett Memorial Scholarship
- Missouri College Guarantee Program
- Missouri College Guarantee PLUS Program
- Missouri Higher Education Academic "Bright Flight" Scholarship

In fiscal year 2006, the legislature appropriated approximately $41 million for these programs.

Effective July 1, 2005, information technology personnel and resources from most executive branch agencies, including DHE, were consolidated and placed under the direction of the state Chief Information Officer in the Office of Administration, Information Technology Services Division. Under the consolidation, DHE maintains ownership of FAMOUS while ITSD provides the technical support to operate the system. This consolidation will be completed July 1, 2006, when personnel from the consolidating departments will become Information Technology Services Division employees and agency technology budgets are fully transferred to the division.

Student information maintained in FAMOUS includes contact information, social security numbers, financial information, college assessment test scores, and other information necessary to determine eligibility. Post-secondary institution users have access to FAMOUS information only on students who have authorized release of information to their particular

institution. DHE staff with access to FAMOUS have access to all student data maintained in the system.

DHE is required to comply with FERPA[1] to protect the privacy of student education records. This federal law requires schools, appropriate state officials, and others to keep information confidential, which would be considered harmful or an invasion of privacy if disclosed. This law covers information maintained in FAMOUS.

Scope and Methodology

To understand the measures taken to ensure confidentiality, integrity and availability of data and the system, we requested, and reviewed when available, FAMOUS policies and procedures, user manuals, and other documents. We also interviewed DHE officials and the ITSD representative for DHE (ITSD official) to determine what information technology and data integrity controls were in place.

We based our evaluation on applicable state, federal, national and international standards and best practices related to information technology controls from the following sources:

- Missouri Adaptive Enterprise Architecture
- National Institute of Standards and Technology
- U.S. Government Accountability Office
- ISACA's Control Objectives for Information and related Technology (COBIT)
- International Organization for Standardization/International Electrotechnical Commission

We requested comments on a draft of our report from the Commissioner of the Department of Higher Education. We conducted our work between December 2005 and February 2006.

Operating Risks Are Not Assessed

Identifying and assessing information security risks are essential steps in determining what controls are required and what level of resources should be expended on controls. Moreover, by increasing awareness of risks, these assessments generate support for the adopted policies and controls, which helps ensure policies and controls operate as intended, according to the U.S. Government Accountability Office. Accepted standards state a risk assessment helps identify potential threats and vulnerabilities, the resulting impact, and the appropriate controls to mitigate the impact and achieve and maintain an acceptable level of risk.

[1] 34 Code of Federal Regulations Part 99.

In 2004, a project risk assessment was performed to identify, assess and control project risks for developing and implementing FAMOUS. However, a risk assessment has not been completed since implementation of the FAMOUS system to identify system operating risks. According to the ITSD official, a risk assessment had not been a priority due to limited staff and the availability of resources. According to accepted standards, the principal goal of an organization's risk management process should be to protect the organization and its ability to perform its mission.

Security Features Leave Student Data and System at Risk

Security must be considered in the design of an information system according to accepted standards. Experience has shown it is very difficult to implement security measures properly and successfully after a system has been developed so these measures should be integrated fully into the design and development of the system, according to the National Institute of Standards and Technology. DHE and ITSD officials implemented the FAMOUS system without many commonly accepted security features. The system has some basic security; however, these features are inadequate and cumbersome. DHE and ITSD staff are working on implementing additional software to manage system security. The ITSD official said the department considered this software during the FAMOUS development process but did not include it during the implementation because staff did not have time to become familiar with and customize the software. This official said the department expects the software to be implemented by the start of the 2006/2007 school year.

The basic security features in FAMOUS consist of access rights granted to user IDs and the use of passwords to authenticate IDs. However, common security features required by accepted standards, including statewide standards in the Missouri Adaptive Enterprise Architecture, are not yet available to help safeguard FAMOUS. These missing security features include:

- A requirement for users to change their passwords the first time they log on to the system.
- A requirement to change passwords on a scheduled basis.
- The capability for users to change passwords themselves; all passwords must be changed by DHE information technology staff.
- A system-required minimum password length.
- Automatic termination of a user session after a specified period of inactivity.
- A limit to the number of concurrent sessions for a single user ID.
- Use of an audit log for producing security reports to identify inappropriate or unusual activity.

Collectively, these user ID, password, and security reporting weaknesses impair DHE's ability to comply with FERPA and ensure the confidentiality of the FAMOUS data.

Knowledge of passwords not limited to individual user

According to accepted standards, access controls such as passwords are key to ensuring only authorized individuals gain access to data. Passwords provide a method of validating a user's identity to establish access rights. Moreover, passwords are most effective when they are kept confidential and limited to an individual user. DHE password management controls are not sufficient to prevent unauthorized access to FAMOUS data. The ITSD official said passwords are maintained for all post secondary institution users in a file on the DHE network where 14 DHE and ITSD employees have access. This list is maintained so employees can help post-secondary institution users. Employees with access to read the password file could use this information to masquerade as another user and gain access to confidential student data without detection.

Documented Policies are Necessary to Ensure Security of Operations

Documentation of all aspects of computer operations and support is important to ensure continuity and consistency. Formalizing operational practices and procedures with sufficient detail helps to eliminate security lapses and oversights, gives new personnel sufficiently detailed instructions, and provides a quality assurance function to help ensure operations will be performed correctly and efficiently, according to accepted standards.

DHE has documented some policies and procedures for the operation of FAMOUS including a user manual. DHE has also developed procedures but has not yet formally documented these procedures and associated policies for the following security controls:

- Data classification
- Rules of behavior
- User IDs and passwords
- Data integrity
- System and data backup

Data classification not documented

A data classification framework is established to define an appropriate set of protection levels and the placement of data in information classes, according to accepted standards. Such a framework examines the sensitivity of both the data to be processed and the system itself to identify when to classify information as confidential, public or other established levels. Sensitivity is generally classified in terms of confidentiality, integrity and availability. Factors such as the importance of the system to the organization's mission and the consequences of unauthorized use of the system or data need to be examined when assessing sensitivity. Accepted standards also state a data

classification framework is necessary to ensure integrity and consistency of all data.

DHE has not documented a framework for data classification, according to DHE and ITSD officials. Student-specific data in FAMOUS must be kept confidential due to FERPA requirements. DHE officials have not documented this guideline as a formal policy statement so it can be conveyed to FAMOUS users. A DHE official said data classification was not documented because all data in FAMOUS relates to student records and must be kept confidential.

FAMOUS users are not informed of responsibilities

Accepted standards state a rules of behavior should be established and made available to every user of the system. The rules of behavior should clearly delineate responsibilities and expected behavior of all individuals with access to the system. These rules should state the consequences of inconsistent behavior or noncompliance. The rules of behavior could also help ensure users are aware of FERPA guidelines.

DHE has not documented the rules of behavior for FAMOUS, according to the ITSD official. Manuals are available for users which document how to use the system, but they do not include what is considered proper use of the system or a statement of the consequences of noncompliance. DHE and ITSD officials said they have not had time to ensure all of the necessary information was in these manuals because FAMOUS was just implemented for the 2005/2006 school year.

In addition to ensuring every user receives a set of rules of behavior, users may be informed of the proper use of the system through a logon banner. The FAMOUS system does not have a logon banner, according to the ITSD official. The Missouri Adaptive Enterprise Architecture requires a logon banner that notifies users, among other points, what is considered the proper use of the system.

No documentation of access controls

Access controls prevent unauthorized people from entering a system and usually require the system to identify and differentiate among users. User accountability requires the linking of activities on an information system to specific individuals and, therefore, requires the system to identify users, according to accepted standards.

DHE staff has established access controls for FAMOUS and ITSD staff has established procedures for maintaining user account access. However, these controls and procedures have not been documented, according to the ITSD official. As noted above, DHE and ITSD officials said the FAMOUS user

manuals lack some necessary information due to the system's recent implementation.

Data integrity controls not documented

Data integrity exists when data agrees with its source and has not been accidentally or maliciously modified, altered or destroyed, according to accepted standards. Integrity is lost if unauthorized changes are made to the data or system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccurate data, fraud, or erroneous decisions.

Data integrity is maintained through field constraints within the FAMOUS software, according to the ITSD official. For example, the system only allows numbers to be entered in numeric fields or ensures certain values entered are within an acceptable range. The ITSD official said these data integrity constraints are not documented outside of the software because she did not know there was a need to do so. According to accepted standards, data integrity management requires an organization to define and document policies and procedures to ensure integrity and consistency of data. This process improves the quality of management decision-making by helping to ensure reliable and secure information is provided.

Backup procedures not documented

Accepted standards state system data should be backed up regularly. In addition, policies should be documented that specify the frequency of backups, the location of stored data, file-naming conventions, media rotation frequency, and method for transporting data offsite.

The ITSD official said the FAMOUS system is automatically backed up nightly. However, these backup procedures have not been documented. The official said since the backups are scheduled to run automatically, DHE and ITSD officials had not seen the need to document the procedures.

Conclusions

DHE and ITSD officials have not taken all necessary measures to fully ensure the confidentiality, integrity, and availability of student records maintained in FAMOUS and to ensure system security. DHE officials do not have assurance appropriate controls are in place to reduce the risks of threats and vulnerabilities to an acceptable level since a current risk assessment has not been performed. The lack of adequate security features over user IDs and passwords and the lack of documented security policies further contribute to an increased risk of confidential data being vulnerable to unauthorized disclosure and use. To provide for the proper protection of FAMOUS, DHE officials should ensure risks have been identified, adequate security features are in place and security controls are documented to facilitate user awareness and compliance with laws and regulations.

Recommendations

We recommend Department of Higher Education officials work with Information Technology Services Division officials to:

1. Perform a risk assessment of the FAMOUS system to ensure the appropriate security controls are in place to mitigate risks.

2. Implement or develop security software for FAMOUS that will allow officials to customize and enhance security configurations.

3. Discontinue maintaining a centralized list of passwords.

4. Document policies and procedures for the following security controls:

    - Data classification framework.
    - Rules of behavior to inform FAMOUS users of their responsibilities and expected behavior when using the system.
    - Maintaining user accounts and the established user access controls.
    - Data integrity rules and constraints.
    - Backup procedures for system and data files.

Agency Comments

1. *Both DHE and ITSD officials agree with this recommendation and the following action has been taken. The ITSD official has completed a risk assessment of the FAMOUS system that has been reviewed and approved by other ITSD officials and DHE officials.*

2. *Both DHE and ITSD officials agree with this recommendation and the following action has been taken. The ITSD official has drafted a PAQ (Project Assessment Quotation) request to be presented to vendors listed on the IT Consulting Services contract (C206014001) for assistance with the installation and setup of Tivoli Access Manager software. The use of this software should address the missing security features noted in the audit report. We plan to have it operational for FAMOUS by August 2006.*

3. *Both DHE and ITSD officials agree with this recommendation but disagree with the following statement from the audit report. "Employees with access to read the password file could use this information to masquerade as another user and gain access to confidential student data without detection." The employees with access to the password file already have access to all student data via their own IDs; therefore, there would be no threat of misuse as stated. However, this practice will be discontinued as soon as the security software is implemented.*

4. *Both DHE and ITSD officials agree with this recommendation and the following action has been taken. Policies have been written for each security control noted in the report and have been reviewed and approved by other ITSD officials and DHE officials.*