



Louisiana State University System
3810 West Lakeshore Drive
Baton Rouge, Louisiana 70808

Office of the President

225 / 578-2111

225 / 578-5524 fax

DATE: April 19, 2005

PM-36

MEMORANDUM TO: Chancellors Cavanaugh, Costonis, Marsala, McDonald, Nunez, O'Keefe, Richardson, Rock, Ryan, Executive Director Bouchard, and Chief Executive Officer Smithburg

SUBJECT: Louisiana State University System Information Security Plan

This document is a coordinated effort of the Offices of the Executive Vice-President, the LSU System Internal Audit, the LSU System Compliance Office, the State of Louisiana Office of Information Technology and campus information technology representatives. The purpose of the policy is to provide guidance to campuses in developing compliance programs that address state and federal regulations involving LSU System information technology systems that are either critical to business continuity in the event of a disaster or which contain protected or restricted information.

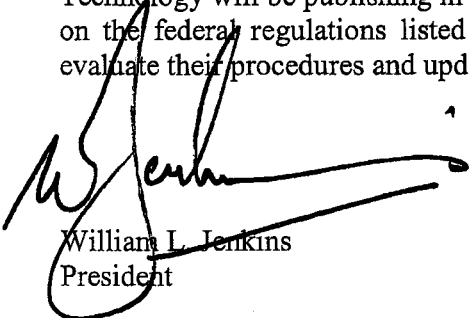
The LSU System Office recognizes that not all LSU System campuses are the same and that not all campus information systems contain protected or restricted information as defined by state or federal regulatory agencies.

Since the release of the HIPAA Security guidelines, industry best practice standards suggest implementation of a "universal" information security program that reasonably meets current and anticipated regulations. The International Standard Organization (ISO) 17799 Standards have been recommended repeatedly. The required regulatory policy statements in this document are based on these standards. Aside from the specificity of HIPAA Security guidelines, regulations are often general and are left open to interpretation. For that reason, this policy implements the HIPAA Security required and addressable standards using the ISO 17799 "best practices" approach.

It is the intent of the LSU System Office to provide flexibility and accountability to each System campus to develop and implement individual campus procedures that comply with the policy statements contained in this PM. An addendum is attached to the policy statements which contain "best practices" suggestions to assist each campus in achieving compliance. These suggestions are not mandatory, nor are they to be interpreted as a directive in a particular

regulation. They are merely suggestions of "best practices" to assist the campuses in carrying out the intent of the policy statements. It will be the decision of the individual campus to include these suggestions in its operational procedures. This decision should be made with the input at a minimum from campus administration, internal audit, budget and finance, and compliance.

This Information Security Plan is considered to be "living" in that it will be continually evaluated to ensure that all LSU System campuses remain in compliance with information security requirements. It is important to note that the Louisiana Office of Information Technology will be publishing in the near future Information Technology Security policies based on the federal regulations listed earlier. LSU System campuses are expected to continually evaluate their procedures and update as needed.



William L. Jenkins
President

Attachment: (1) Table of Contents and Chapters 1-12
(2) Glossary
(3) References

cc: System Offices (w/o attachments)

PM-36: Attachment 1
TABLE OF CONTENTS AND CHAPTERS 1-12

SECTION	PAGE
Chapter 1 – Securing Systems, Hardware, Software and Peripherals	5
A. Subunit 1 – Purchasing and Installing Hardware	5
1. Policy Statement 1.1.1 – Security Standards and Guidelines	5
2. Policy Statement 1.1.2 – Specifying Information Security Requirements for New Systems	5
3. Policy Statement 1.1.3 – Installation, Upgrade and Testing of Hardware, Systems and Equipment	5
B. Subunit 2 – Cabling, UPS, Printers, and Modems	5
1. Policy Statement 1.2.1 – Supplying Continuous Power to Critical Equipment	5
2. Policy Statement 1.2.2 – Managing High Availability Systems	5
3. Policy Statement 1.2.3 – Using Fax Machines/Fax Modems	5
4. Policy Statement 1.2.4 – Using Modems/ISDN/DSL Connections	5
5. Policy Statement 1.2.5 – Using Centralized, Networked or Stand Alone Printers	5
6. Policy Statement 1.2.6 – Securing Network Cabling	6
C. Subunit 3 – Consumables	6
1. Policy Statement 1.3.1 – Using Removable Storage Media Including Diskettes and CDs.....	6
D. Subunit 4 – Working Off Campus or Using Outsourced Processing	6
1. Policy Statement – 1.4.1 – Contracting or Using Outsourced Processing	6
2. Policy Statement – 1.4.2 – Using of Laptop/Portable Computers, Portable Electronic Devices and the Removal of Equipment Off LSU System Campuses.....	6
3. Policy Statement – 1.4.3 – (Teleworking) or Working from Home Or Other Off-Site Location	6
E. Subunit 5 – Hardware and System Documentation	6
1. Policy Statement 1.5.1 – Maintaining and Using Hardware and System Documentation	6
Subunit 6 – Other Hardware Issues	7
2. Policy Statement 1.6.1 – Destruction and/or Reuse of Equipment	7
3. Policy Statement 1.6.2 – Recording, Reporting and Correcting System Faults	7
4. Policy Statement 1.6.3 – Logon and Logoff from Computer	7
5. Policy Statement 1.6.5 – Damage to Equipment	7
II. Chapter 2 – Controlling Access to Information and Systems	8
A. Subunit – Controlling Access to Information and Systems	8
1. Policy Statement 2.1.1 – Managing Access Control Standards	8
2. Policy Statement 2.1.2 – Managing User Access	8
3. Policy Statement 2.1.3 – Securing Unattended Workstations	8
4. Policy Statement 2.1.4 – Managing Network Access Controls	8

SECTION	PAGE
5. Policy Statement 2.1.5 – Managing Application Access Control	8
6. Policy Statement 2.1.6 – Managing Passwords	8
7. Policy Statement 2.1.7 – Unauthorized Physical Access to Security	8
8. Policy Statement 2.1.8 – Monitoring System Access and Use	8
9. Policy Statement 2.1.9 – Managing System Access	8
10. Policy Statement 2.1.10 – Controlling Remote User Access	10
11. Policy Statement 2.1.11 – Emergency Access	10
III. Chapter 3 – Processing Information and Documents	10
A. Subunit 1 – Networks	10
1. Policy Statement 3.1.1 – Configuring Networks	10
2. Policy Statement 3.1.2 – Managing the Network	10
3. Policy Statement 3.1.3 – Defending Network Information Against Malicious Attacks	10
B. Subunit 2 – System Operations and Administration	10
1. Policy Statement 3.2.1 – Appointing System Administrators	10
2. Policy Statement 3.2.2 – Controlling Data Distribution	10
3. Policy Statement 3.2.3 – Permitting Third Party Access	10
4. Policy Statement 3.2.4 – Ensuring Information Integrity	10
5. Policy Statement 3.2.5 – Commissioning Facilities Management	10
C. Subunit 3 – E-mail and the Worldwide Web	11
1. Policy Statement 3.3.1 – Downloading Files and Information from the Internet	11
2. Policy Statement 3.3.2 – Sending Electronic mail (Email) and /or Other Forms of Digital Communication	11
3. Policy Statement 3.3.3 – Receiving Electronic Mail and/or Any Other Form of Digital Communication	11
4. Policy Statement 3.3.4 – Misdirected Information by E-mail and/or Any Other Form of Digital Communication	11
5. Policy Statement 3.3.5 – Website Maintenance	11
D. Subunit 4 – Data Management	11
1. Policy Statement 3.4.1 – Transferring and Exchanging Data	11
2. Policy Statement 3.4.2 – Managing Data Storage	11
E. Subunit 5 – Backup, Recovery and Archiving	12
1. Policy Statement 3.5.1 – Restarting or Recovering the System	12
IV. Chapter 4 – Purchasing and Maintaining Commercial Software	13
A. Subunit 1 – Purchasing and Installing Software	13
1. Policy Statement 4.1.1 – Using Licensed Software	13
B. Subunit 2 – Software Maintenance and Upgrade	13
1. Policy Statement 4.2.1 – Supporting Application Software	13
2. Policy Statement 4.2.2 – Disposing of Information System Software	13
V. Chapter 5 – Developing and Maintaining Custom Software	14
A. Subunit 1 – Controlling Software Code	14

SECTION	PAGE
1. Policy Statement 5.1.1 – Managing Operational Program Libraries	14
2. Policy Statement 5.1.2 – Managing Program Source Libraries	14
3. Policy Statement 5.1.3 – Controlling Deployment of Software	14
B. Subunit 2 – Software Development	14
1. Policy Statement 5.2.1 – Software Development	14
C. Subunit 3 – Testing and Training Environments	14
1. Policy Statements 5.3.1 – The Use of Protected Data for Testing	14
2. Policy Statements 5.3.2 – New System Training	14
VI. Chapter 6 – Complying with Regulatory and Policy Requirements	15
A. Subunit 1 – Complying with Regulatory Obligations	15
1. Policy Statement 6.1.1 – Awareness of Regulatory Obligations	15
2. Policy Statement 6.1.2 – Copyright Compliance	15
3. Policy Statement 6.1.3 – Computer Misuse: Regulatory Safeguards	15
VII. Chapter 7 – Business Continuity Planning	16
A. Subunit 1 – Management of Business Continuity Plan (BCP)/Disaster Recovery Plan (DRP)	16
1. Policy Statement 7.1.1 – Initiating the BCP/DRP	16
2. Policy Statement 7.1.2 – Assessing the BCP/DRP Security Risk	16
3. Policy Statement 7.1.3 – Testing the BCP/DRP	16
4. Policy Statement 7.1.4 – Training and Staff Awareness of the BCP/DRP	16
VIII. Chapter 8 – Addressing Personnel Issues Relating to Security	17
A. Subunit 1 – Contractual Documentation	17
1. Policy Statement 8.1.1 – Preparing Conditions of Employment	17
2. Policy Statement 8.1.2 – Employing/Contracting New Staff	17
3. Policy Statement 8.1.3. – External Suppliers/Other Vendors Contracts	17
4. Policy Statement 8.1.4 – Non-Disclosure Agreements.....	17
B. Subunit 2 – Personnel Information Security Responsibilities	17
1. Policy Statement 8.2.1 – Passwords and PIN Numbers	17
C. Subunit 3 – Employment Termination	17
1. Policy Statement 8.3.1 – Staff Resignations	17
2. Policy Statement 8.3.2 – Procedures for Staff Leaving Employment	17
IX. Chapter 9 – Training and Staff Awareness	18
A. Subunit 1 – Awareness	18
1. Policy Statement 9.1.1 – Awareness for Temporary Staff	18
2. Policy Statement 9.1.2 – Security Information Updates to Staff	18
B. Subunit 2 – Training	18
1. Policy Statement 9.2.1 – Information Security Training on New Systems	18

SECTION	PAGE
2. Policy Statement 9.2.2 – New LSU System Faculty, Staff, and Student Training in Information Security	18
X. Chapter 10 – Physical Security	19
A. Subunit 1 – Campus Security	19
1. Policy Statement 10.1.1 – Preparing Campus for Placement of Computers	19
XI. Chapter 11 – Protecting for, Detecting and Responding to Information Security Incidents	20
A. Subunit 1 – Reporting Information Security Incidents	20
1. Policy Statements 11.1.1 – Defending Against Unauthorized or Criminal Activity	20
2. Policy Statements 11.1.2 – Security Incident Procedures	20
B. Subunit 2 – Investigating Information Security Incidents	20
1. Policy Statement 11.2.1 - Investigating the Cause and Impact of Information Security Incidents	20
2. Policy Statement 11.2.2 – Responding to Information Security Incidents	
XII. Chapter 12 – Classifying Information and Data	21
A. Subunit 1 – Setting Classification Standards	21
1. Policy Statement 12.1.1 – Defining Information	21
2. Policy Statement 12.1.2 – Classifying Information	21
3. Policy Statement 12.1.3 – Characteristics and Handling of Protected Information	21
4. Policy Statement 12.1.4 – Characteristics and Handling of Restricted Information	

I. Chapter 1—Securing Systems, Hardware, Software and Peripherals

A. Subunit 1—Purchasing and Installing Hardware

1. **Policy Statement 1.1.1—Security Standards and Guidelines**
Each LSU System campus shall develop and implement written technical standards to ensure the confidentiality, integrity, and availability of the data stored on its information systems. All equipment and software purchased or developed shall adhere to these standards. These standards shall be reviewed periodically.
2. **Policy Statement 1.1.2 Specifying Information Security Requirements for New Systems**
All proposed information systems to be purchased with LSU System campus funds (including donations, grants etc.) shall be submitted to the person designated by the IT department for review for adherence to IT department security standards, and approval prior to purchase.
3. **Policy Statement 1.1.3—Installation, Upgrade and Testing of Hardware, Systems and Equipment**
All hardware installations shall be planned and related parties impacted by the installation notified and given the opportunity to comment prior to the proposed installation date. All equipment, systems, software, upgrades and patches shall be fully and comprehensively tested and authorized by management prior to being converted to a “live” environment. The extent of planning and testing shall be reasonable given the size and complexity of the installation to ensure successful implementation with a minimal disruption of operation.

B. Subunit 2—Cabling, UPS, Printers, and Modems

1. **Policy Statement 1.2.1—Supplying Continuous Power to Critical Equipment**
All information systems identified as critical to LSU System campus operations shall be protected by an uninterruptible power supply adequate to provide continuity of services and/or orderly shutdown to preserve data integrity.
2. **Policy Statement 1.2.2—Managing High Availability Systems**
Each LSU System campus Information Technology department shall identify those systems which require a high degree of availability and ensure continued operation during power outages and hardware faults.
3. **Policy Statement 1.2.3—Using Fax Machines/Fax Modems**
Protected or restricted information shall only be faxed when more secure methods are not available.
4. **Policy Statement 1.2.4—Using Modems/ISDN/DSL Connections**
Protected or restricted information shall only be sent via non-LSU System campus network lines when more secure methods are not feasible. In that event, additional precautions e.g. encryption of data, virtual private network, etc., shall be employed to ensure against unauthorized interception and/or disclosure of protected information.
5. **Policy Statement 1.2.5—Using Centralized, Networked, or Stand Alone Printers**
Protected or restricted information shall not be sent to a network printer in an unsecured area without appropriate physical safeguards or an authorized person present to safeguard this information during and after printing.

6. **Policy Statement—1.2.6—Securing Network Cabling**
All cabling in LSU System campus networks shall be secured to prevent unauthorized interception or damage.

C. **Subunit 3—Consumables**

1. **Policy Statement 1.3.1—Using Removable Storage Media Including Diskettes and CDs**
All protected or restricted information stored on removable media, including diskettes and CDs, shall be kept in a safe, secure environment in accordance with the manufacturers' specifications when not in use. The removal of protected or restricted information from campus premises shall require specific authorization from the campus designated official.

D. **Subunit 4—Working Off Campus or Using Outsourced Processing**

1. **Policy Statement 1.4.1—Contracting or Using Outsourced Processing**
Individuals responsible for commissioning outsourced computer processing of protected or restricted information shall ensure the services used are from companies that operate in accordance the campus' information security standards which include a Business Associate Agreement or similar document that communicates the expectation of compliance with these standards and the remedies available in the instance of non-compliance.
2. **Policy Statement 1.4.2—Use of Laptop/Portable Computers, Portable Electronic Devices and the Removal of Equipment Off LSU System Campuses**
Laptops and other portable computing devices issued to LSU System campus employees shall not be used for activities unrelated to LSU organizational goals. The designated campus official shall document who is in possession of each device and that the individual understands his responsibility for the confidentiality, integrity and availability of the information on said device. Each LSU System campus employee who is assigned a portable or mobile computing device shall be responsible for ensuring that data stored on that device is properly backed up, that the operating system is patched in a timely fashion, and where applicable, anti-virus software with current virus data file (including spyware detection and firewalls) is installed and running continuously. In addition, only authorized personnel shall be permitted to take any equipment belonging to the LSU System campus off the premises and are responsible for its security at all times.
3. **Policy Statement 1.4.3—(Teleworking) or Working from Home or Other Off-Site Location**
LSU System campuses which allow teleworking or working from home shall establish procedures that ensure the confidentiality, integrity and availability of protected data accessed during any teleworking session.

E. **Subunit 5—Hardware and System Documentation**

1. **Policy Statement 1.5.1—Maintaining and Using Hardware and System Documentation**
Up to date hardware and system documentation, such as operator manuals or technical information provided by suppliers or vendors, shall be readily available to staff who are authorized to support or maintain the system.

F. Subunit 6—Other Hardware Issues

1. **Policy Statement 1.6.1—Destruction and/or Reuse of Equipment**
IT equipment and/or media owned by LSU System campuses shall only be disposed of by authorized personnel in accordance with the National Industrial Security Program Operations Manual (DOD standard 5220.22M) and the Louisiana Office of Information Technology policy. IT equipment and/or media owned by a LSU System campus which is to be reassigned to another employee or reused shall be evaluated as to whether protected or restricted information needs to be purged in accordance with the above standard prior to reassignment and/or reuse or disposal.
2. **Policy Statement 1.6.2—Recording, Reporting and Correcting System Faults**
Each campus shall develop and implement a procedure for documenting and responding to significant information system incidents that impact multiple users.
3. **Policy Statement 1.6.3—Logon and Logoff from Computer**
Logon procedures shall be strictly followed and users leaving their screen unattended must secure their workstation or logoff. All information systems storing protected or restricted information shall incorporate technical methods to secure unattended workstations in unsecured areas to prevent unauthorized use.
4. **Policy Statement 1.6.4—Damage to Equipment**
All deliberate damage to or theft of LSU System campus IT property shall be reported to the Security Officer and appropriate law enforcement as soon as it is discovered.

II. Chapter 2—Controlling Access to Information and Systems

A. Subunit 1—Controlling Access to Information and Systems

1. **Policy Statement 2.1.1—Managing Access Control Standards**
Each LSU System campus shall ensure that all access to information systems is based on the lowest level of privilege needed to perform one's job.
2. **Policy Statement 2.1.2—Managing User Access**
Access to any LSU System campus information system shall be authorized by the owner and/or campus designated official(s). Each faculty, staff, student and contractor shall be assigned a unique user ID. When generic IDs are required by operational necessity, each campus shall develop procedures to prevent abuse. For audit purposes, such access, including the appropriate access rights or privileges, and a record of the authorization shall be maintained for six years after the access is terminated.
3. **Policy Statement 2.1.3—Securing Unattended Workstations**
Precautions shall be taken to prevent unauthorized changes to unattended equipment.
4. **Policy Statement 2.1.4—Managing Network Access Controls**
Access to LSU System campus information systems networks shall be strictly controlled to prevent unauthorized access. Each campus' IT department shall develop procedures and standards for securing network electronics against unauthorized tampering.
5. **Policy Statement 2.1.5—Managing Application Access Control**
The LSU System campus procedure for authorizing supervisor-level access shall require approval from the designated campus IT authority.
6. **Policy Statement 2.1.6—Managing Passwords**
All LSU information systems that use passwords as the primary method of user authentication shall require that all user accounts be password protected with non-null weak passwords and require all users to change passwords on a periodic basis. The IT department of the LSU System campus shall develop and/or adopt standards for password length, password change interval and password complexity that are appropriate for the system being protected. These standards shall be reviewed periodically. These standards shall not be any less restrictive than that specified by the State of Louisiana Office of Information Technology policy.
7. **Policy Statement 2.1.7—Unauthorized Physical Access Security**
Physical access to server rooms and network infrastructure closets shall be protected using all reasonable and appropriate safeguards. Strong authentication and identification techniques shall be used when they are available and can be reasonably deployed.
8. **Policy Statement 2.1.8—Monitoring System Access and Use**
All LSU information systems that contain protected or restricted information shall be configured to log any and all information necessary to detect and record attempts of unauthorized access and system errors, to the extent that the logging facility exists and is capable. These logs with significant activity shall be examined in a timely fashion by staff determined as qualified by the campus IT department. Security incidents shall be reported to the Security Officer for appropriate action and follow up.
9. **Policy Statement 2.1.9—Managing System Access**
Access controls for information systems shall be set in accordance to the value and classification of the information assets being protected.

10. **Policy Statement 2.1.10—Controlling Remote User Access**
Each LSU System campus shall develop a procedure for authorizing remote access of LSU information systems by LSU faculty, staff, students and vendors. The campus IT department shall establish standards to ensure accurate authentication of remote users and the integrity and confidentiality of the information transmitted.

11. **Policy Statement 2.1.11—Emergency Access**
All LSU System campuses shall develop and implement a procedure to provide access to electronic information on an emergency basis (i.e., an employee is incapacitated and another employee must enter the system to continue his job function). For audit purposes, each instance of such access provision shall be documented and shall be maintained on file for a period of no less than six years, if the information accessed is protected information.

III. Chapter 3—Processing Information and Documents

A. Subunit 1—Networks

1. **Policy Statement 3.1.1—Configuring Networks**
All LSU System information system networks shall be designed and configured to deliver high availability, confidentiality, and integrity to meet business needs.
2. **Policy Statement 3.1.2—Managing the Network**
Each LSU System campus shall ensure that those responsible for managing the campus' network and preserving its integrity in collaboration with the individual system owners does so in accordance to the campus' IT department standards and job descriptions.
3. **Policy Statement 3.1.3—Defending Network Information Against Malicious Attack**
Each LSU System campus shall develop and implement procedures to adequately configure and safeguard its information system hardware, operation and application software, networks and communication systems against both physical attack and unauthorized network intrusion. All servers and work stations shall run anti-virus software (including spyware detection and firewalls) while connected to LSU network infrastructure. In the event that the system will not operate properly with the anti-virus software, appropriate information security safeguards shall be instituted.

B. Subunit 2—System Operations and Administration

1. **Policy Statement 3.2.1—Appointing System Administrators**
Each LSU System campus shall appoint systems administrators who demonstrate the qualifications established by the campus' IT department to manage the information technology systems and oversee the day to day security of these systems.
2. **Policy Statement 3.2.2—Controlling Data Distribution**
While appropriate data and information must be made available to authorized personnel when required, access to such data and information by all other persons shall be prohibited using appropriate technical controls.
3. **Policy Statement 3.2.3—Permitting Third Party Access**
Each LSU System campus shall develop and implement a procedure in which third party access granted to LSU System information systems that contain protected or restricted information is documented by a Business Associate Agreement or similar document that specifies the access to be granted and the controls to be used by both parties to ensure confidentiality, integrity and availability of the data.
4. **Policy Statement 3.2.4—Ensuring Information Integrity**
All LSU System campuses shall develop and implement procedures to ensure that the integrity of electronic protected or restricted information is maintained in the event of processing errors, system failure, human errors, natural disasters and deliberate acts.
5. **Policy Statement 3.2.5—Commissioning Facilities Management**
Any facilities management company engaged by a LSU System campus shall be expected to comply with LSU System Information Security policies and to execute a Business Associate Agreement or similar document that communicates the performance expected and the remedies available in the instance of non compliance.

C. Subunit 3—E-mail and the World-wide Web

1. **Policy Statement 3.3.1—Downloading Files and Information From the Internet**
Each LSU System campus IT department shall develop standards and guidelines to ensure information, software and media downloaded from the Internet does not jeopardize its operations or the security of information systems.
2. **Policy Statement 3.3.2—Sending Electronic Mail (E-Mail) and/or Other Forms of Digital Communication**
Each LSU System campus shall develop procedures that require all email and/or any other form of digital communication generated by its information systems that contains protected or restricted information, including data attachments, shall only be permitted after confirming that such action is consistent with the restriction specified by the security classification of the information being sent. In addition, the file shall be scanned for the possibility of a virus or other malicious code. In no case shall protected or restricted information be sent outside the LSU information infrastructure without taking precautions to ensure the confidentiality and integrity of the information.
3. **Policy Statement 3.3.3—Receiving Electronic Mail and/or Any Other Form of Digital Communication**
Each LSU System campus shall develop and implement standards and procedures that will ensure that malicious code is not delivered to or executed on LSU information systems by receiving email and/or any other form of digital communication.
4. **Policy Statement 3.3.4—Misdirected Information by E-Mail and/or Any Other Form of Digital Communication.**
Each LSU System campus shall develop and implement procedures that ensure that emails and/or any other form of digital communication that contain protected or restricted information, including attachments, are correctly addressed and only being sent to appropriate persons. This procedure shall include a mechanism in which the misdirected communication is correctly delivered without the content being viewed any further than is necessary to identify the appropriate recipient and deleted from the mistaken recipient's computer system.
5. **Policy Statement 3.3.5—Website Maintenance**
Each LSU System campus shall develop and implement a procedure which ensures LSU System websites that contain protected or restricted information are protected from unauthorized intrusion.

D. Subunit 4—Data Management

1. **Policy Statement 3.4.1—Transferring and Exchanging Data**
All restricted or protected information shall only be transferred outside of LSU networks, or copied to other media, when the confidentiality and integrity of the data can reasonably be assured.
2. **Policy Statement 3.4.2—Managing Data Storage**
All data stored on LSU information systems shall be managed to ensure the confidentiality, integrity and availability of the data.

E. Subunit 5—Backup, Recovery and Archiving

1. **Policy Statement 3.5.1—Restarting or Recovering the System**
All LSU information systems that contain protected or restricted information shall be protected by adequate backup and system recovery procedures. These procedures shall ensure the integrity of data files, especially when these files were replaced by more recent files.

IV. Chapter 4—Purchasing and Maintaining Commercial Software

A. Subunit 1—Purchasing and Installing Software

- 1. Policy Statement 4.1.1—Using Licensed Software**
Each LSU System campus shall make every effort to ensure that all terms and conditions of End User License Agreements (EULA) are strictly adhered to in order to comply with applicable laws and to ensure ongoing vendor support.

B. Subunit 2—Software Maintenance and Upgrade

- 1. Policy Statement 4.2.1—Supporting Application Software**
All LSU application software shall be supported to ensure that the campus' business is not compromised. Every effort shall be made to resolve software problems efficiently and within an acceptable time period.
- 2. Policy Statement 4.2.2—Disposing of Information System Software**
Disposal of information systems software shall not occur unless the disposal is authorized by the appropriate campus official, the information systems software is no longer required, and its related data can be archived and will not require restoration in the future.

V. Chapter 5—Developing and Maintaining Custom Software

A. Subunit 1—Controlling Software Code

1. **Policy Statement 5.1.1—Managing Operational Program Libraries**
Each LSU System campus shall implement a procedure in which only authorized staff may access operational program libraries.
2. **Policy Statement 5.1.2—Managing Program Source Libraries**
Each LSU System campus shall implement a procedure in which only authorized staff may access program source libraries.
3. **Policy Statement 5.1.3—Controlling Deployment of Software Code During Software Development**
All changes to systems, source code and operational program libraries shall be properly authorized and tested before moving to the live environment.

A. Subunit 2—Software Development

1. **Policy Statement 5.2.1—Software Development**
Each LSU System campus shall implement a procedure in which all software developed for systems identified as critical to campus operations must always follow a formal managed development process appropriate for the size and scope of the system.

B. Subunit 3—Testing and Training Environments

1. **Policy Statement 5.3.1—The Use of Protected Data for Testing**
Each LSU System campus shall implement a procedure that requires adequate controls for the security of protected or restricted data when used in the testing of new systems or system changes.
2. **Policy Statement 5.3.2—New System Training**
Each LSU System campus shall implement a procedure in which users and technical staff are trained in the functionality and operations of all new systems.

VI. Chapter 6—Complying with Regulatory and Policy Requirements

A. Subunit 1—Complying with Regulatory Obligations

- 1. Policy Statement 6.1.1— Awareness of Regulatory Obligations**
All LSU System campuses shall develop and implement procedures to inform employees of their regulatory responsibilities in relation to the use of computer based information and data.
- 2. Policy Statement 6.1.2—Copyright Compliance**
All LSU System campuses shall develop and implement procedures to inform employees of their obligation to comply with applicable copyright laws.
- 3. Policy Statement 6.1.3—Computer Misuse: Regulatory Safeguards**
Each LSU System campus shall implement a procedure by which employees are informed of regulatory changes concerning computer misuse, as it directly impacts their job duties.

VII. Chapter 7—Business Continuity Planning

A. Subunit 1—Management of Business Continuity Plan (BCP)/Disaster Recovery Plan (DRP)

- 1. Policy Statement 7.1.1—Initiating the BCP/DRP**
Each LSU System campus shall develop and implement a written Business Continuity Plan (BCP) and/or Disaster Recovery Plan (DRP) to ensure the continuation of key information systems services in the event that these services are disrupted. A current copy of this Plan and any amendments shall be submitted to the LSU System Office of the Executive Vice-President for review and to be kept on file.
- 2. Policy Statement 7.1.2—Assessing the BCP/DRP Security Risk**
Each LSU System campus shall conduct a formal risk assessment in order to determine the requirements for the BCP/DRP. Each LSU System campus shall review its risk assessment after each emergency and at least every three years.
- 3. Policy Statement 7.1.3—Testing the BCP/DRP**
Each LSU System campus shall implement a procedure in which the BCP is tested at least annually. Results of such testing, i.e. a disaster recovery drill, shall be submitted to the LSU System Office of the Executive Vice President. The BCP/DRP shall be produced in the appropriate format to guarantee its availability during an emergency.
- 4. Policy Statement 7.1.4—Training and Staff Awareness of the BCP/DRP**
All appropriate LSU staff shall receive training in the use of the BCP/DRP and in their continuity plan roles.

VIII Chapter 8—Addressing Personnel Issues Relating to Security

A. Subunit 1—Contractual Documentation

1. **Policy Statement 8.1.1—Preparing Conditions of Employment**
All LSU System campuses shall require employees to acknowledge compliance with information security policies as it is applicable to their job duties.
2. **Policy Statement 8.1.2—Employing/Contracting New Staff**
Each LSU System campus shall verify that new employees are eligible to participate in university business and its affiliated programs.
3. **Policy Statement 8.1.3—External Suppliers/other Vendors Contracts**
All LSU System campuses' suppliers/vendors who handle protected or restricted information shall acknowledge compliance with the campus' information security procedures prior to the delivery of services.
4. **Policy Statement 8.1.4—Non-Disclosure Agreements**
All LSU System campuses shall require all third parties to execute non-disclosure agreements e.g. Business Associate Agreements when engaged in the use or disclosure of information classified as protected or restricted.

B. Subunit 2—Personnel Information Security Responsibilities

1. **Policy Statement 8.2.1—Passwords and PIN Numbers**
All LSU System campus faculty, staff and students are expected to treat passwords as private and highly confidential.

C. Subunit 3—Employment Termination

1. **Policy Statement 8.3.1—Staff Resignations**
All LSU System campuses shall ensure that the appropriate Security Officer is notified of all employee terminations and that access to LSU System campus information systems is revoked. If in the judgment of the appropriate campus official, it is determined that an employee represents a risk to the security of LSU System campus information, all access shall be terminated immediately.
2. **Policy Statement 8.3.2—Procedures for Staff Leaving Employment**
All LSU System campuses shall develop and implement a procedure to ensure that all LSU System campus property previously assigned to a departing employee is returned, and also that all keys, access cards and forms of employee identification are returned.

IX. Chapter 9—Training and Staff Awareness

A. Subunit 1—Awareness

1. **Policy Statement 9.1.1—Awareness for Temporary Staff**
All LSU System campus temporary staff with access privileges to the campus networks shall acknowledge compliance with the campus' Information Security policies prior to beginning work with the campus.
2. **Policy Statement 9.1.2—Security Information Updates to Staff**
Updates on Information Security awareness shall be provided to the staff on an evolving, ongoing basis as events warrant.

B. Subunit 2—Training

1. **Policy Statement 9.2.1—Information Security Training on New Systems**
Each LSU System campus faculty, staff and students shall complete information security training appropriate for their job function. If the user's job responsibilities change, then the user's training requirements shall be reassessed and new training must occur, if required.
2. **Policy Statement 9.2.2—New LSU System Faculty, Staff and Student Training in Information Security**
All new LSU System campus faculty, staff and students shall receive mandatory Information Security training appropriate for their job or educational function within thirty calendar days of their start date.

X. Chapter 10—Physical Security

A. Subunit 1—Campus Security

1. **Policy Statement 10.1.1.—Preparing Campus for Placement of Computers**
All LSU System campus information systems hardware and media that contain protected or restricted information shall be located in areas that are protected from physical intrusion, theft, fire, flood, excessive temperature/humidity or other hazards.

XI. Chapter 11— Protecting For, Detecting and Responding to Information Security Incidents

A. Subunit 1—Reporting Information Security Incidents

1. **Policy Statement 11.1.1.—Defending Against Unauthorized or Criminal Activity**
Each LSU system campus shall develop and implement procedures to defend campus networks and information systems that contain protected or restricted information against vandalism, unauthorized physical intrusion, unauthorized access, denial of service, virus attack, spyware/malware or criminal activity.
2. **Policy Statement 11.1.2—Security Incident Procedures**
All LSU system campuses shall develop and implement procedures requiring that all suspected or actual information security incidents as defined by the campus' IT department are promptly reported to the Information Security Officer or campus designee.

B. Subunit 2—Investigating Information Security Incidents

1. **Policy Statement 11.2.1—Investigating the Cause and Impact of Information Security Incidents**
All LSU system campuses shall develop and implement procedures for the thorough investigation of information security incidents as defined by the campus' IT department. Investigators shall be properly trained and qualified. Results of the investigation shall be thoroughly documented in a security incident report to be kept on file for at least six years. The report shall include any and all recommendations to prevent a recurrence of similar incidents.
2. **Policy Statement 11.2.2—Responding to Information Security Incidents**
All LSU System campuses shall develop and implement procedures for the response to information system security incidents as defined by the campus' IT department. Every effort shall be made to mitigate the adverse impact on the confidentiality, integrity and availability of data, and to preserve any evidence that could be used in the investigation of the incident.

XII. Chapter 12—Classifying Information and Data

A. Subunit 1—Setting Classification Standards

1. **Policy Statement 12.1.1—Defining Information**
All LSU System campuses shall maintain a database of their information assets to include rankings of each asset with regard to confidentiality, integrity, availability and criticality to operations.
2. **Policy Statement 12.1.2—Classifying Information**
Each LSU System campus shall adopt a method to classify its electronic protected or restricted information according to the level of confidentiality, sensitivity, value and criticality. This method shall not be less restrictive than the method defined by Louisiana state law and/or the State of Louisiana Office of Information Technology.
3. **Policy Statement 12.1.3—Characteristics and Handling of Protected Information**
Protected information is information that shall have extraordinary controls over its use and disclosure due to the sensitivity of its content. Examples of Protected information include, but are not limited to: employment records, medical records, student records, personal financial records (or other individually identifiable information), research data, trade secret information and classified government information. Protected information shall not be transmitted outside the confines of the LSU System campus network without the use of appropriate safeguards to preserve its confidentiality and integrity. Protected information shall not be shared with contractors or other business associates without an approved agreement in place governing the use, handling and disclosure of the confidential information. Any unauthorized use and/or disclosure of protected information shall be reported to the Security Officer immediately. Should it become necessary to disclose protected information, in order to provide requested services to an individual or comply with existing laws and regulations, the information disclosed shall be the minimum necessary to perform the service or comply with the legal requirement.
4. **Policy Statement 12.1.4—Characteristics and Handling of Restricted Information**
Restricted information is information of such a sensitive nature that access is limited to those individuals designated by management as having a need to know. Examples of restricted information include, but are not limited to ongoing investigations, pending litigation, psychology notes and disciplinary action. All LSU System campuses shall take appropriate measures to ensure that restricted information is not disclosed to anyone other than to those individuals designated by management.

Best Practices Suggestions

In addition to the Policy Statements, the LSU System Information Security Plan Committee offers the following “best practices” suggestions to assist the campuses in complying with the regulatory information security mandates.

Best Practices Suggestions for Chapter 1, Section A, Subunit 1:

1. Standards should be reviewed no less frequently than every 3 years and revised if necessary to ensure adherence to industry best practices. All standards documents should include version number and date of adoption for audit purposes. In the event that already existing systems do not meet the newly revised standards, then they may be grandfathered until a replacement or update can be planned and implemented.
2. The IT policy adherence review should be scalable to the size and complexity of the purchase. The campus IT department may at its own discretion set monetary and/or other parameters to determine appropriate levels of review and/or develop and publish a pre-approved list of items which are commonly purchased.

Best Practices Suggestions for Chapter 1, Section B, Subunit 2:

1. The sender of the protected or restricted information and the intended recipient should agree to the fax transmittal prior to sending.
2. The sender of the protected or restricted information via modem/ISDN/DSL connections and the intended recipient should agree to the transmission prior to sending.
3. Each LSU System campus Information Technology department should establish standards for standards should be reviewed periodically, as with other IT department standards. This review should occur no less than once every 3 years and be revised if necessary to ensure the standards are in accordance with industry best practices. The campus IT department may, at its discretion “grandfather” older network installations, provided those installations were done in accordance with existing standards at the time of installation and/or good engineering practice, and the installation adequately serves the needs of the campus.
4. To prevent abuse of network facilities, all network connections should be monitored or secured.

Best Practices Suggestions for Chapter 1, Section D, Subunit 4

1. All protected or restricted information stored on a portable or mobile computing device should be encrypted.

Best Practices Suggestions for Chapter 1, Section F, Subunit 6:

1. Significant information system incidents should be corrected by qualified staff or third party technicians.
2. Equipment owned, leased or licensed by the LSU System campus should be supported by appropriate maintenance facilities and/or qualified engineers.

Best Practices Suggestions for Chapter 2, Section 1, Subunit A

1. Access records should be considered confidential and safeguarded as such.
2. Precautions to prevent tampering with workstations should include: limiting access to server rooms, locking wiring closets, incorporating idle time outs for work stations, and password controlled screensavers.
3. Access to operating system supervisor and/or administrator commands should be restricted to those persons who are authorized to perform systems administration/management functions.
4. HIPAA Privacy reasonable safeguards pertaining to passwords should be included in password management standards where appropriate. The password management standard review should occur no less frequently than every three years and revised to incorporate advances in technology.
5. For effective auditing and monitoring, each campus should establish a threshold (or clipping level) to limit the amount of logging information generated.

Best Practices Suggestions for Chapter 3, Section A, Subunit 1

1. All anti-virus data files should be updated no less frequently than monthly.
2. All adequately tested operating system patches should be applied in a timely fashion.

Best Practices Suggestions for Chapter 3, Section B, Subunit 2

1. For effective auditing and monitoring, all third party user accounts should expire or be renewed no more than one year from the date they were created or renewed.
2. Systems' operations processes should be formally planned, authorized, scheduled and documented to ensure that necessary processes are successfully run and completed, and that unauthorized processes are not performed. Changes to routine systems operations should be fully tested and approved before being implemented.
3. In order to accurately document and mitigate information security incidents, all LSU campus information system clocks should be synchronized regularly to the extent possible.
4. Only qualified staff or third party technicians should repair information system hardware faults.
5. If possible, transaction and processing reports should be reviewed regularly to detect processing errors, system failure, human errors, natural disasters and deliberate acts that may affect the integrity of electronic protected information.

Best Practices Suggestions for Chapter 3, Section C, Subunit 3

1. Only personnel who demonstrate the qualifications established by the campus IT department should modify the campus website, especially if it contains protected information. These modifications should be documented for audit purposes

Best Practices Suggestions for Chapter 4, Section B, Subunit 2

1. Each LSU System campus should implement a procedure in which patches to resolve software bugs are only applied when verified and authorized by the campus IT department.
2. Each LSU System campus should develop and implement a procedure in which system faults are recorded and reported to those responsible for system support/maintenance.

Best Practices for Chapter 5, Section A, Subunit 1

1. Amendments to operational program libraries should only be made using a combination of technical access controls and strong procedures operated under dual control.
2. Amendments to program source libraries should only be made using a combination of technical access controls and strong procedures operated under dual control.

Best Practices Suggestions for Chapter 5, Section B, Subunit 2

1. Emergency amendments to software are discouraged, except in cases in which management has designated a circumstance as "critical". Any amendments should strictly follow agreed upon change control procedures.
2. All proposed new software development or system enhancements should be business driven and supported by an approved business case. Ownership (Responsibility for) such development or enhancements should be assigned to the business owner of the system.
3. Each LSU System campus should implement a procedure in which proper segregation of duties should be ensured for all areas dealing with system development, system operation, or system administration.

Best Practices Suggestions for Chapter 5, Section C, Subunit 3

1. Each LSU system campus should maintain a suitable test environment for all systems identified as critical to campus operations.
2. Each LSU System campus should implement a procedure in which new systems are tested for capacity, peak loading, and stress testing. The new system should demonstrate a level of performance and resilience which meets or exceeds the technical and business needs and requirements of the campus.
3. Normal system testing procedures for each LSU System campus should incorporate a period of parallel running, when deemed necessary, prior to the new or amended system being acceptable for use in the live environment.

Best Practices Suggestions for Chapter 5 in General

1. Each LSU System campus should implement a procedure in which all new and enhanced systems are fully supported by comprehensive and recent documentation. New or upgraded systems should not be introduced into the live environment unless supporting documentation is available.
2. Each LSU System campus should ensure that all vendor developed software meets the User Requirements Specifications and offers appropriate product support.

Best Practices Suggestions for Chapter 6

1. Regulatory responsibilities of employees in relation to use of computer based information should be included in any "Terms of Employment" and the campus' Code of Conduct.

Best Practices Suggestions for Chapter 8, Section A, Subunit 1

1. Compliance with information security policies should be included in any "Terms of Employment" and the Campus' Code of Conduct.

2. **Lending of keys, both physical and electronic, should be prohibited by each LSU System campus. In the event that access to an area or information secured by a physical or electronic key is required by an individual without such key, that individual should be accompanied and supervised by someone who has been issued such a key.**
3. **Employees should be notified that non-compliance with information security policies can result in immediate disciplinary action, up to and including termination of employment and/or enrollment.**

Best Practices Suggestion for Chapter 10

Each LSU System campuses should develop and implement processes to record the identity of individuals who improperly gain physical access to secure information technology areas.

Best Practices Suggestions for Chapter 11, Section A, Subunit 1

1. **Each LSU system campus should adhere to industry recognized best practices when collecting and protecting evidence from information systems so that criminal perpetrators can be prosecuted to the fullest extent of the law.**

Best Practices Suggestions for Chapter 12

1. **At a minimum, the classification system should incorporate four levels. Examples of these levels are, in increasing order of restrictions, Public, Internal, Protected and Restricted.**
2. **Public information can be defined as information with no restrictions and can be released to the general public in accordance with university policy.**
3. **Internal information can be defined as information regarding the internal business and education operations of the LSU System and its campuses. Examples of internal information include but are not limited to emails, memos, management and operational reports. Internal information may not be disclosed without approval of the management of the appropriate department of the LSU System campus.**

PM-36: Attachment 2

GLOSSARY

Business Associate Contract Addendum— See Attached

Business Continuity Plan (BCP) -- plan and preparations directed towards either the immediate recovery of systems critical to the function of the business, or to the ability of the business to operate in the temporary absence of important systems

Digital Communication--electronic exchange of information (e.g., e-mail, cellular phones, instant messaging)

Disaster Recovery Plan (DRP) -- a plan and preparations directed towards the resumption of business and the recovery of systems after catastrophic loss of important systems. A disaster recovery plan is generally concerned with longer time frames than a business continuity plan. Sometimes also referred to as a business resumption plan.

Louisiana Office of Information Technology (OIT) -- Provides the electronic government structure for the executive branch of state government as directed by ACT 772 - 2001 Regular Session
<http://www.legis.state.la.us/bills/byinst.asp?sessionid=01RS&billtype=SB&billno=455>

National Industrial Security Program Operations Manual (DOD standard 5220.22M)--This manual is issued in accordance with the National Industrial Security program (NISIP). The Manual prescribes requirements, restrictions, and other safeguards that are necessary to prevent unauthorized disclosure of classified information and to control authorized disclosure of classified information released by U.S. Government Executive Branch Departments and Agencies to their contractors. The Manual also prescribes requirements, restrictions, and other safeguards that are necessary to protect special classes of classified information, including *restricted data, formerly restricted data, intelligence sources and methods information, sensitive compartmented Information, and Special Access Program information*. These procedures are applicable to licenses, grantees, and certificate holders to the extent legally and practically possible within the constraints of applicable law and the Code of Federal Regulations.
http://www.dss.mil/ise/nispom_0195.htm

Owner of Information Systems--Internal and permanent staff member with the competence required to evaluate and classify a certain number of systems for which he is accountable. Information system owners grant access rights to the information systems they own and ensure that adequate security measures are taken to protect this information, and to guarantee its integrity and confidentiality. Even though the overall responsibility falls entirely to information system owners, they have the power to delegate certain tasks to employees under their direction.

Parallel Running-- The process of running a new or amended system simultaneously with the old system to confirm that it functions correctly before going live.

Protected or Restricted Information--information that shall have extraordinary controls over its use and disclosure due to the sensitivity of its content. Examples of Protected information include, but are not limited to: employment records, medical records, student records, personal financial records (or other individually identifiable information), research data, trade secret information and classified government information. Restricted information is information of such a sensitive nature that access is limited to those individuals designated by management as having a need to know. Examples of restricted information include, but are not limited to ongoing investigations, pending litigation, psychology notes and disciplinary action.

Segregation of Duties--a method of working where tasks are assigned to different members of staff to reduce the occurrence of error or fraud.

Server Rooms-- rooms that contain computers/devices which provide information or services to computers on a network.

Attachment: Business Associate Contract Addendum

**PM-36: Attachment 3
REFERENCES**

Federal Regulations

1. **FDA (US Food and Drug Administration)-21 CFR, Chapter 1, Part 11 Electronic Records; Electronic Signatures**
http://www.access.gpo.gov/nara/cfr/waisidx_04/21cfr11_04.html
2. **Gramm-Leach-Bliley-16 CFR Part 313 Privacy of Consumer Financial Information; Final Rule**
<http://www.ftc.gov/os/2000/05/65fr33645.pdf>

<http://www.ftc.gov/privacy/glbact/glb-faq.htm>
3. **HIPAA Security Rules-45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule**
<http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.pdf>
4. **NIH (National Institutes of Health)-45 CFR, Part 46, Subpart A**
<http://www.hhs.gov/ohrp/policy/index.html#certificate>
5. **Office Management and Budget- CIRCULAR NO. A-130, Revised, (Transmittal Memorandum No. 4)** <http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html>

State Regulations

1. **Title 44, Public Records and Recordors**
<http://www.legis.state.la.us/lss/lss.asp?folder=64>
2. **Louisiana State Office of Information Technology Security Policies**
<http://www.doa.louisiana.gov/oit/index.htm>
Best Practices Suggestions References
3. **International Organization for Standardization (ISO 17799) Information Technology**
<http://www.iso.ch/iso/en/prods-services/popstds/informationsecurity.html>
4. **National Institute of Standards and Technology (NIST) Computer Security Division**
<http://csrc.nist.gov/pcig/index.html>

Business Associate Contract Addendum

On this ____ day of _____, 200__, the undersigned, [Name of Covered Entity] ("Covered Entity") and [Name of Business Associate] ("Business Associate") have entered into this "Business Associate Contract Addendum" ("Addendum") for the purposes herein set forth.

1. Business Associate Relationship

(a) Covered Entity and Business Associate are parties to that certain contract, denominated "[Name of underlying contract], dated _____ ("the Agreement"), and pursuant to which Business Associate is performing functions or tasks on behalf of Covered Entity.

(b) Covered Entity is bound by the regulations implementing the Health Insurance Portability and Accountability Act of 1996, P. L. 104-191 ("HIPAA"), 45 C.F.R. Parts 160 and 164 ("the Privacy Rule"). The intent and purpose of this Addendum is to comply with the requirements of the Privacy Rule, including, but not limited to, the Business Associate contract requirements at 45 C.F.R. §§ 164.502(e) and 164.504(e).

(c) In the performance of this Agreement, Business Associate is performing functions on behalf of Covered Entity which meet the definition of "Business Associate Activities" in 45 C.F.R. § 160.103, and therefore Business Associate is a "Business Associate" of Covered Entity.

(d) In order for Business Associate to perform its obligations under the Agreement, Covered Entity must disclose to Business Associate certain Protected Health Information (as defined in 45 C.F.R. §160.103) that is subject to protection under HIPAA and the Privacy Rule.

NOW, THEREFORE in consideration of the mutual promises and covenants contained herein, and in furtherance of the mutual intent of the parties to comply with the requirements of the Privacy Rule, the parties agree as follows:

2. Definitions

(a) **Protected Health Information.** "Protected Health Information" shall have the meaning found in 45 C.F.R. '160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity. "Protected Health Information" may also be referred to as "PHI".

(b) **Secretary.** "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

Terms used in this Addendum, but not otherwise defined herein, shall have the same meaning as in the Privacy Rule.

3. Obligations and Activities of Business Associate

(a) Business Associate agrees not to use or disclose PHI other than as stated in this Agreement this Addendum or as Required By Law.

(b) Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for in this Addendum. Business Associate acknowledges receipt of a copy of Covered Entity's policies and procedures for safeguarding PHI, and agrees to implement substantially identical safeguards for PHI in its possession.

(c) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Addendum.

(d) Business Associate agrees to report promptly to Covered Entity any use or disclosure of the PHI not provided for by this Addendum of which it becomes aware.

(e) Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides PHI received from, or created or received by Business Associate on behalf of Covered Entity, agrees to the same restrictions and conditions that apply through this Addendum to Business Associate with respect to such information.

(f) Business Associate agrees to provide access, at the request of Covered Entity, and in a prompt and timely manner, to PHI in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements of 45 C.F.R. § 164.524.

(g) Business Associate agrees to make any amendment(s) to PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 C.F.R. § 164.526 at the request of Covered Entity or an Individual.

(h) Business Associate agrees to make its internal practices, books, and records, including policies and procedures relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Covered Entity available to the Covered Entity, or to the Secretary, in a prompt and timely manner or as designated by the Secretary, for purposes of determining Covered Entity's compliance with the Privacy Rule.

(i) Business Associate agrees to document such disclosures of PHI as would be required for Covered Entity to respond timely to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528.

(j) Business Associate agrees that, in requesting PHI from Covered Entity, and in using or disclosing PHI to others, only the Minimum Necessary information shall be requested, used or disclosed.

4. HIPAA Security Requirements Effective April 20, 2005

Business Associate agrees to:

(1) implement and document, as set forth in 45 C.F.R. § 164.316, Administrative Safeguards, Physical Safeguards and Technical Safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity, as required by 45 C.F.R. Part 164, Subpart C, and specifically, but not exclusively, including the following:

(a) Ensure the confidentiality, integrity, and availability of all electronic protected health information the Business Associate creates, receives, maintains, or transmits on behalf of LSU;

(b) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

(c) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the HIPAA Privacy Regulations;

(d) Ensure compliance with this Section by its workforce;

(2) ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement and document reasonable and appropriate Administrative Safeguards, Physical Safeguards and Technical Safeguards, including at least the requirements set forth in this Section for Business Associate;

(3) report to LSU any Security Incident of which it becomes aware;

(4) make its policies and procedures, and documentation required by this Section relating to such safeguards, available to the Secretary and to LSU for purposes of determining the Business Associate's compliance with this Section; and

(5) authorize termination of the contract or other relationship by LSU if LSU determines that the Business Associate has violated a material term of the contract or this Business Associate Addendum.

For the purposes of this Section, the following terms have the meaning assigned to them below:

Administrative Safeguards means administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the Business Associate's workforce in relation to the protection of that information, as more particularly set forth in 45 C.F.R. § 164.308.

Physical Safeguards means physical measures, policies, and procedures to protect Business Associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion, as more particularly set forth in 45 C.F.R. § 164.310.

Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Technical Safeguards means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it, as more particularly set forth in 45 C.F.R. § 164.312.

Terms used in this Section but not defined herein shall have the meaning assigned to such terms by 45 C.F.R. Part 164, Subpart C, specifically including, but without limitation, 45 C.F.R. § 164.304.

5. Permitted Uses and Disclosures by Business Associate

(a) Except as otherwise prohibited by law or limited in this Addendum, Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in this Agreement, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity or the Privacy Rule, including, but not limited to the following:

(1) Use or disclose PHI for proper management and administration or to carry out the legal responsibilities of the Business Associate, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached. Entities to which Business Associate discloses PHI for the purpose of management and administration of the Business Associate shall be deemed "agents" or "subcontractors" of Business Associate, within the meaning of Section 3(e) of this Addendum.

(2) Use PHI to provide Data Aggregation services to Covered Entity as permitted by 45 C.F.R. § 164.504(e) (2) (i) (B).

6. Obligations of Covered Entity

(a) Covered Entity shall notify Business Associate of any limitation(s) in its Notice of Privacy Practices in accordance with 45 C.F.R. § 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI. Business Associate acknowledges that it has received a copy of Covered Entity's Notice of Privacy Practices, and agrees to comply with all limitations on use and disclosure of PHI contained therein.

(b) Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

(c) Covered Entity shall notify Business Associate of any changes in Covered Entity's Notice of Privacy Practices.

7. Term and Termination of Agreement

(a) Term. The Term of this Addendum shall be effective as of the date of execution by the last party executing same, and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.

(b) Termination for Cause. Notwithstanding any other provisions of this Agreement, upon Covered Entity's knowledge of a material breach by Business Associate of the terms of this Addendum, Covered Entity shall either:

(1) Provide an opportunity for Business Associate to cure the breach. Covered Entity may terminate this Agreement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity;

(2) Immediately terminate this Agreement if Business Associate has breached a material term of this Addendum and cure is not possible; or

(3) If neither termination nor cure is feasible in the sole discretion of Covered Entity, Covered Entity shall report the violation to the Secretary.

(c) Effect of Termination.

(1) Except as provided in paragraph (2) of this section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all PHI received

from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. Business Associate shall not retain copies of any PHI. This provision shall also apply to PHI that is in the possession of subcontractors or agents of Business Associate.

(2) In the event that Business Associate determines that returning or destroying the PHI is not feasible, Business Associate shall notify Covered Entity of this determination and its reasons. If Covered Entity agrees that return or destruction of PHI is not feasible, Business Associate shall extend the protections of this Addendum to such PHI and limit further uses and disclosures, for so long as Business Associate maintains such PHI. This provision shall also apply to PHI that is in the possession of subcontractors or agents of Business Associate.

8. Miscellaneous

(a) Regulatory References. Any reference in this Addendum to a section in the Privacy Rule means the section as in effect or as amended.

(b) Formal Amendment and Deemed Amendment. The Parties agree to take such action as is necessary to formally amend this Addendum from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191. Regardless of the execution of a formal amendment of this Addendum, the Addendum shall be deemed amended to permit the Covered Entity to comply with HIPAA and the Privacy Rule, as the same may be hereafter amended or interpreted.

(c) Survival. The respective rights and obligations of Business Associate under Section 6 (c) of this Addendum entitled "Effect of Termination" shall survive the termination of this Addendum and/or the Agreement.

(d) Interpretation. Any ambiguity in this Addendum shall be resolved to permit Covered Entity to comply with the Privacy Rule.

(e) Material Breach of Addendum as Breach of Agreement. Any material breach of this Addendum by Business Associate shall constitute a material breach of the Agreement, and shall entitle Covered Entity to any of the remedies provided in the Agreement, in addition to the remedies provided herein.

(f) Provisions of Addendum to Control. In the event of any conflict between the provisions of this Addendum and any of the other provisions of the Agreement, including any renewal, extension or modification thereof, the provisions of this Addendum shall control.

(g) Ownership of PHI. The PHI to which Business Associate, or any agent or subcontractor of Business Associate has access under the Agreement shall be and remain the property of Covered Entity.

(h) Indemnification and Contribution. Each party to this Addendum shall indemnify and hold the other harmless from any and all claims, liability, damages, costs and expenses, including attorney's fees and costs of defense and attorney's fees, resulting from the action or omission of the other party. In the event that any liability, damages, costs and expenses arise as a result of the actions or omissions of both parties, each party shall bear such proportion of such liability, damages, costs and expenses as are attributable to the acts or omissions of such party.

(i) Injunctive Relief. Notwithstanding any rights or remedies provided for in this Agreement, Covered Entity retains all rights to seek injunctive relief to prevent or stop the inappropriate use or disclosure of PHI directly or indirectly by Business Associate, or any agent or subcontractor of Business Associate.

(j) Attorney's Fees. If any legal action or other proceeding is brought for the enforcement of this Addendum or in connection with any of its provisions, the prevailing party shall be entitled to an award for the attorney's fees and costs incurred therein in addition to any other right of recovery.

(k) Severability. If any clause or provision of this Addendum is held to be illegal, invalid or unenforceable under any present or future law, the remainder of this Addendum will not be affected thereby. It is the intention of the parties that, if any such provision is held to be illegal, invalid or unenforceable, there will be substituted in lieu thereof a provision as similar in terms to such provision as is possible which is legal, valid and enforceable.

(l) Waiver of Provisions. Failure by either party at any time to enforce or require the strict performance of any of the terms and conditions of this Agreement shall not constitute a waiver of such terms or conditions or modify such provision or in any manner render it unenforceable as to any other time or as to any other occurrence. Any specific waiver by either party of any of the terms and conditions of this Agreement shall be considered a one-time event and shall not constitute a continuing waiver. Neither a waiver nor any failure to enforce shall in any way affect or impair the terms or conditions of this Agreement or the right of either party to avail itself of its remedies.

(m) Choice of Law. To the extent not preempted by HIPAA or the Privacy Rule, the Laws of the State of Louisiana shall govern this Addendum.

(n) Notices. Any notice, demand or communication required or permitted to be given by any provision of this Addendum shall be in writing and will be deemed to have been given when actually delivered (by whatever means) to the party designated to receive such notice, or on the next business day following the day sent by overnight courier, or on the third (3rd) business day after the same is sent by certified United States mail, postage and charges prepaid, directed to the addresses noted below, or to such other or additional address as any party might designate by written notice to the other party, whichever is earlier.

Notices required by this Addendum shall be sent as follows:

Covered Entity:

Business Associate:

[Name]
[Institution]
[Address]
[City, State Zip Code]

[Name]
[Institution]
[Address]
[City, State Zip Code]

Copy to:

Copy to:

[Name]
[Institution]
[Address]
[City, State Zip Code]

[Name]
[Institution]
[Address]
[City, State Zip Code]

THUS DONE AND SIGNED on the date first written above:

[Name of Covered Entity]:

By:

Title:

[Name of Business Associate]:

By:

Title:

**TAYLOR, PORTER,
BROOKS & PHILLIPS**
L.L.P.

MEMORANDUM

DATE: April 23, 2004
TO: Lisa LeBoeuf
FROM: H. Evans Scobee
RE: Applicability of Gramm-Leach-Bliley to LSU

Introduction

Pursuant to our discussions of last week I am expanding on the opinion letter furnished to LSU by Michael Dufilho on April 13, 2004.

For the reasons that follow, we believe that LSU is subject to the Gramm-Leach-Bliley Act ("GLBA") [15 U.S.C.A. §§ 6802 *et seq.*; 16 C.F.R. Part 313 (Privacy) and 16 C.F.R. Part 314 (Safeguards)] since we conclude that LSU is a "financial institution" within the meaning of the GLBA, and is not subject to any blanket exemption. However, with respect to student financial records only, LSU will be deemed to be in compliance with the privacy provisions of the GLBA to the extent LSU in compliance with the provisions of the Family Educational Rights and Privacy Act ("FERPA") [20 U.S.C. § 1232g; 34 CFR Part 99] .

The GLBA also has certain provisions known as "Safeguards," similar to the Security Rules under HIPAA, designed to protect the security and integrity of financial information. With respect to the Safeguards provisions, LSU must comply with these provisions with respect to all financial records, student and non-student.

Background of the Gramm-Leach-Bliley Act

The GLBA, like HIPAA, was not intended primarily as privacy or security legislation. The original intention was to remove certain restrictions placed on financial, brokerage and insurance institutions.. These restrictions were placed on the financial, brokerage and insurance institutions by the Glass-Steagall Act of 1933 and the Bank Holding Company Act of 1956, as amended in 1982. These provisions restricted banks, brokerages and insurance companies from entering each other's lines of business, and greatly restricted the ability of these institutions to merge and combine. The GLBA removed many of these restrictions in an effort to "modernize" the financial services industry, but the original Senate bill contained none of the privacy protections contained in the final act. Because of concerns regarding the potential misuse of consumer financial information across these traditionally separate industries and institutions, the privacy and security provisions were added to the "modernization" provisions of GLBA in the House, and were enacted into law in the final legislation. Like HIPAA, the scope of the GLBA's privacy protections is quite broad, bringing within its purview many institutions not traditionally considered to be "financial institutions."

Scope of the GLBA

The GLBA applies to "the treatment of nonpublic personal information about consumers by the financial institutions listed in paragraph (b) of this section" (16 C.F.R. § 313.1 (a)).

16 C.F.R. § 313.1 (b) defines a “financial institution” as follows:

An entity is a “financial institution” if its business is engaging in a financial activity as described in Section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. 1843(k), which incorporates by reference activities enumerated by the Federal Reserve Board in 12 CFR 211.5(d) and 12 CFR 225.28.

The same section of the GLBA regulations contains the “exemption” for institutions of higher learning:

Any institution of higher education that complies with the Federal Educational Rights and Privacy Act (“FERPA”), 20 U.S.C. 1232g, and its implementing regulations, 34 CFR part 99, and that is also a financial institution subject to the requirements of this part, shall be deemed to be in compliance with this part if it is in compliance with FERPA.

It should be noted that this provision does not “exempt” institutions of higher education from GLBA, but rather merely allows FERPA compliance to be “deemed” compliant with GLBA. Also, the exemption only applies to “this part,” meaning 16 C.F.R. Part 313, containing the Privacy protections. The Safeguards provisions (similar to the HIPAA Security regulations) are in 16 C.F.R. Part 314 and this “exemption” does not apply to those requirements. As a consequence, to the extent GLBA applies to LSU, as we believe it does, the Safeguards rules will have to be followed with respect to all financial information, student and non-student.

A subsequent section of the implementing regulations further refines the definition of “financial institution”:

Financial institution means any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)). An institution that is significantly engaged in financial activities is a financial institution.

16 C.F.R. § 313.3(k)(1); emphasis supplied

The “financial activities” enumerated in 12 U.S.C. 1843(k) include:

- lending, exchanging, transferring, investing for others, or safeguarding money or securities
- insuring, guaranteeing, or indemnifying against loss, harm, damage, illness, disability, or death
- Engaging in an activity that the Federal Reserve Board has determined to be closely related to banking. [12 U.S.C.A. §1843(k)(4); 12 C.F.R. § 225.28]. For example:
 - Extending credit and servicing loans
 - Collection agency services
 - Real estate and personal property appraising
 - Check guaranty services
 - Credit bureau services
 - Real estate settlement services
 - Leasing real or personal property (on a nonoperating basis for an initial lease term of at least 90 days)

If LSU is “significantly engaged” in any of these activities, then, under the applicable provisions of GLBA and its implementing regulations, LSU is a financial institution, and is subject to the

requirements of the Privacy rules and the Safeguards rules promulgated on the authority of the GLBA.

Colleges and Universities as “financial institutions” under GLBA

The first inquiry, then, is whether LSU is “significantly engaged” in activities that would bring it within the above quoted definition of a “financial institution.” From the standpoint of the Federal Trade Commission (“FTC”), the answer to that inquiry is “yes.”

The FTC’s Position

Before publication of the final GLBA privacy rule in May of 2000, a number of commenters to the proposed rule urged the FTC to specifically exempt institutions of higher education from GLBA because they are not “financial institutions,” and because the privacy concerns addressed by GLBA are already addressed by the provisions of FERPA applicable to institutions of higher education. The FTC responded to these comments in the preamble to the final rule.

The FTC agreed that FERPA offered sufficient privacy protections with respect to students’ records, but flatly rejected the suggestion that colleges and universities are not “financial institutions”:

The Commission also received several comments from colleges and universities and their representatives requesting that institutions of higher education be excluded from the definition of financial institution. The Commission disagrees with those

commenters who suggested that colleges and universities are not financial institutions. Many, if not all, such institutions appear to be significantly engaged in lending funds to consumers. However, such entities are subject to the stringent privacy provisions in the Federal Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. 1232g, and its implementing regulations, 34 CFR part 99, which govern the privacy of educational records, including student financial aid records. The Commission has noted in its final rule, therefore, that institutions of higher education that are complying with FERPA to protect the privacy of their student financial aid records will be deemed to be in compliance with the Commission's rule.

65 Fed. Reg. 33646 at 33648; emphasis supplied

Analysis of the FTC's Position

The FTC's position is based upon the premise that almost all institutions of higher education are involved, in some manner, in making or servicing loans to students or their parents to cover the costs of higher education. Under the provisions of 12 U.S.C.A. § 1843(k)(4)(A), lending money is an activity that is "financial in nature," and under 16 C.F.R. § 313.1 (b) and 16 C.F.R. § 313.3(k)(1), if LSU is "significantly engaged" in making such student loans, LSU would meet the statutory and regulatory definition of a "financial institution" under GLBA.

Under the GLBA's implementing regulations [16 C.F.R. §313.3], the following businesses are also deemed to be "significantly engaged in financial activities":

- A retailer that extends credit by issuing its own credit card directly to consumers

- A career counselor that specializes in providing career counseling services to individuals who are seeking employment with a financial organization
- A business that prints and sells checks for consumers, either as its sole business or as one of its product lines
- A business that regularly wires money to and from consumers
- A check cashing business

As you can see, the regulations include within the definition of “financial institution” many businesses and activities that one would not ordinarily associate with the financial services industry.

The final rule does not define “significantly engaged,” despite several comments to the proposed rule that the lack of a more precise definition left businesses uncertain whether GLBA would govern their activities. The FTC provides some guidance in the rules in the forms of “examples” of conduct that does or does not meet the “significantly engaged” test, some of which are contained in the bulleted list above. As you can see, the examples are not particularly useful when analyzing a university’s conduct., but I have included those examples that might have applicability to LSU.

One exception, however, relates to the issuance of a credit card by a retailer, which renders the retailer “significantly engaged” in financial activity, versus a retailer which merely accepts cards issued by others, which does not. I am given to understand that LSU issues a “Tiger Card,” but for what purpose, I do not know. If the card is proprietary to LSU and has a

credit, debit or other financial or monetary function, it is likely this alone would be sufficient for LSU to be deemed a “financial institution.”

Our understanding of the situation is that LSU is involved in the business of extending financial aid to students and their families on a regular basis, and is, therefore lending or extending credit on a regular basis. This activity, without more, would bring LSU within the definition of a “financial institution,” and subject the university to the requirements of GLBA. If LSU engages in any of the other activities enumerated in the regulations as substantial engagement in financial activities, it will be subject to GLBA without regard to the provision of financial aid to students and their families.

Therefore, unless some judicial modification of the FTC’s position is available, LSU, like virtually every other institution of higher education, will be subject to GLBA.

Judicial Challenges to FTC Positions under GLBA

No reported case deals with a challenge to the FTC’s determination that “most, if not all” colleges and universities are “financial institutions” under GLBA. One case deals with a challenge to the FTC’s informal ruling that certain attorneys were “financial institutions” under GLBA. While the court in that case allowed the challenge to go forward, in the course of the discussion of the applicability of GLBA to lawyers, it reviewed the process by which the FTC included, and then partially “exempted” colleges and universities from the GLBA.

In *New York State Bar Ass'n v. F.T.C.*, 276 F.Supp.2d 110 (D.D.C., 2003), the District Court for the District of Columbia considered a challenge by the New York State Bar Association and the American Bar Association to a letter ruling by the FTC stating that attorneys engaged in certain tax planning and advising activities were “financial institutions” under GLBA, and declining to grant attorneys a *de minimus* exemption despite the fact that confidentiality of clients’ information was already regulated by Bar Association rules. In holding that the FTC had not properly considered the NYSBA and ABA’s position in the matter, the court contrasted the unreasoned action of the FTC with respect to the NYSBA’s and ABA’s requests with the reasoned decision to grant an “exemption” to GLBA-governed universities that comply with FERPA. Although the propriety of the FTC’s actions with respect to universities was not before the court, the deferential language with which the court discusses the manner in which the FTC dealt with institutions of higher learning leaves little doubt that, at least in that court, a *Chevron*¹ challenge to the FTC’s action with respect to universities would be unlikely to succeed.

In light of the deference afforded to agencies’ rulemaking authority, especially when done after public notice and an opportunity to comment, we do not believe a challenge to the

¹ A *Chevron* challenge is an attack on an agency’s rulemaking, based upon the factors set out by the Supreme Court in *Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc.*, 467 U.S. 837, 104 S.Ct. 2778, 81 L.Ed.2d 694 (1984). The test is two-fold. First, a court considers whether Congress spoke directly to the question at issue: if so, “that is the end of the matter, for the court, as well as the agency, must give effect to the unambiguously expressed intent of Congress.” *Id.* at 842-43, 104 S.Ct. 2778. If, however, the statute is unclear, “the question for the court is whether the agency’s answer is based on a permissible construction of the statute.” *Id.* at 843, 104 S.Ct. 2778. In answering that question, “considerable weight should be accorded to an executive department’s construction of a statutory scheme it is entrusted to administer.” *Id.* at 844, 104 S.Ct. 2778.

FTC's position with respect to applicability of GLBA to colleges and universities would be successful.

Conclusion

The preamble to the final privacy rule makes it abundantly clear that the FTC intends that virtually every university that makes, sponsors or services student loans or other financial aid to students or their families will be subject to the GLBA. This position was taken by the agency after consideration of numerous public comments suggesting that colleges and universities should be specifically exempt from GLBA. In light of the requirements of FERPA with respect to students' educational records, including financial records, FERPA compliance will be "deemed" to be GLBA compliance. Additionally, a number of examples of activities in which LSU may be engaged have been specifically ruled by the commission to render the university "substantially engaged in financial activities," and therefore subject to GLBA, irrespective of any participation in financial aid to students or their families. None of the exceptions in the statute or the rules are applicable to LSU. For the reasons stated above, we do not believe that the agency's rulemaking could be challenged successfully.

As a consequence of this, it is our opinion that LSU is subject to the provisions of GLBA and its implementing Privacy and Safeguards regulations, with the sole exception that LSU's compliance with FERPA will be "deemed" to comply with the GLBA's privacy requirements. This exception, however, would only apply to records that are subject to FERPA. All records and information, whether or not subject to FERPA, would have to comply with the Safeguards rule.

Our opinion is based in large measure upon our understanding that LSU is, in fact, involved in the provision of financial aid to its students and their families, or in the servicing or administration of financial aid provided by State and Federal programs. If our understanding is incorrect, then whether LSU is subject to GLBA will depend on whether it is engaged in the other activities enumerated in the regulation which would render LSU “significantly engaged in financial activities.”

If you have any questions or comments, please do not hesitate to contact me..