Proceedings of the 14th Colloquium for Information Systems Security Education
Baltimore Marriott Inner Harbor
Baltimore, Maryland June 7 - 9, 2010

A Study of the Current Use of Information Security Plans at Colleges and Universities

W.V. Maconachy, PhD. *Fellow of ISC*^{2} & Peter Starland, *Capitol College*

Abstract - Recent reports and testimonies to the U. S. Congress have brought into the public eye the massive extent to which U. S. information systems are penetrated by hackers and cyber spies. One recent report provided evidence that U. S. based university information systems are being used by cyber spies as collection and dissemination points for the fruits of their labors. These discoveries are leading to increased federal information security regulations. This report examines the current state of the use of systematic, well-formulated information security plans by colleges and universities. The findings of this first-look study indicate that federal regulations are prompting increased development of information security plans and accountability within U. S. universities and colleges. However, there appears no uniform methodology of format currently employed by American colleges and universities in developing those information security plans. This study reviews current federal regulations motivating the use of information security planning and presents a well-tested information security plan format for consideration and use by colleges and universities.

Index terms – information security plans, information security policies, colleges, universities, cyber security education, information assurance curriculum, information assurance education.

I. Introduction

According to Ken Pappas, vice president/marketing, Top Layer Networks, West-borough schools have a very difficult time with cyber security. "They face the question of how to make their networks open but secure, and struggle with this all of the time" [1]. In years past, colleges and universities attempted to secure their systems through a process of self-regulation. The recent explosion in cyber security breaches as found in FBI IC3 2008 Internet Crime Report noted that, "From January 1, 2008 – December 31, 2008, there were 275,284 complaints filed online with the Internet Crime Complaint Center (IC3). This is a 33.1% increase compared to 2007 when 206,884 complaints were received" [2]. In our opinion, this increased public awareness of the vulnerabilities posed by the internet resulted in two things (1) a marked increase in cyber security awareness in academic institutions, and (2) a host of new federal and state cyber security regulations, to which colleges and universities must respond. This paper explores the current state of the response from colleges and universities to these two factors.

The classic dilemma faced by all academic institutions is access versus controls. In an academic environment a balance must be obtained between the need for total computer security, the need for openness, and the need to conduct research. This is a dilemma also faced by the U.S. government in its efforts to become more transparent when dealing with the public. Therefore, in searching for possible solutions addressing the scope, sequence and content for a college information systems security plan the authors looked closely at current federal solutions.

A. Purpose

This study investigates progress to date in achieving uniform college and university information security plans. For the purposes of this study, information security plan is defined as: a comprehensive college wide policy and education approach for ensuring the security across information technology systems. A critical component to a college information security plan is its implementation. The study also seeks to research and report common practices in implementing campus information security plans.

B. Methodology

The authors of this study incorporated the following methodologies into this research effort:

- Conducted Internet searches for actual college information security plans,
- Consulted with EDUCAUSE,
- Sought guidance and work done to date in campus computer security with selected practitioners,
- Conducted searches of federal sites for regulations, laws, and guidance in preparing information security plans.

C. Delimitations

The scope of study for this paper is limited to U. S. colleges and universities. A major portion of the literature search was conducted by searching open source, online information. Internet search for posted campus IT security plans yielded less than 21 documents online. Of those 14 were selected at random as representational of those posted documents.

D. Hypothesis

There is a lack of uniformity and commonality in breadth, scope, and content in college and university information security plans as compared to the rigor required for Federal Information Systems Management Act (FISMA) reporting.

E. Background

A review of several university information security plans indicated that, in most cases, the college planning was in response to the Financial Services Modernization Act (FSMA) of 1999, also known as the Gramm Leach Bliley Act, 15 U.S.C. Section 6801 [3]. Colleges and universities are able to use this act as an IT security guideline because the Federal Trade Commission ruled that this act applies to institutions of higher education. In addition, when protecting personal student information, these institutions are also bound by the Family Educational Rights and Privacy Act (FERPA) of 1974 [4]. Finally, colleges are also required to be in compliance with the Health Insurance Portability and Accountability Act (HIPAA) of 1996, which safeguards student health information [5]. These recent federal mandates appear to be driving colleges away from self regulation to a model of legislative compliance.

Beyond the emerging federal regulatory requirement regarding university information systems, a recent report to congress portrays a more compelling reason for universities to increase their vigilance in the development and use of information security plans. In an October 2009 Wall Street Journal article, Siobhan Gorman reported on the results of the U. S. – China Economic and Security Review Commission Report. Gorman cited the following results of the Commission's study:

> "They [cyber spies] selected at least eight U. S. computers outside the company, including two at unidentified universities, as a drop point for the stolen data before sending it over seas. The high Internet traffic volume on university networks provides excellent cover" [6].

One of the more complicated issues in dealing with university systems, as noted previously in the Gorman article, is the shear size of the system and all the subsystems across any given campus. As noted in Table 1 Appendix A, a systems computer security plan must take in to account the interrelationships between the subsystems in the overall university information systems context [7]. On some campuses, this requires coordination and harmonization between varieties of systems owners. An example of this system/subsystem integration could be found in a large-scale CAD-CAM system used mostly by engineering departments. Such systems allow for multiple users using multiple access points to make substantial, and often subtle, changes to ongoing systems-type engineering projects. If project managers fail to implement rigorous information systems security controls, such as authentication and system integrity, ongoing product verification and audit become virtually impossible.

While there are no guidelines specifically developed for colleges in meeting the cyber security requirements of the previously cited regulations, the federal government does provide a framework for protecting federal systems. This comprehensive framework was mandated by Federal Information Security Management Act (FISMA), and prepares federal agencies to prove accountability with regards to cyber security practices and procedures [8]. According to FISMA, "The purpose of the system security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system" [9]. For the foreseeable future, the majority of college and universities may never be expected to develop information security plans with the rigor required by FISMA. The implementation guidance provided by the National Institute for Standards and Technology (NIST) could serve as an excellent guide for college and university information security plans. However, for colleges currently engaged in or planning to access and process federal governed information within or on their systems, implementing FISMA based security planning requirements will most likely become mandatory.

There are several sources of valuable information available for use by universities for planning, developing and implementing campus system security plans. Microsoft provides an excellent commercial source for organizations to develop a network security plan [10]. For institutions planning on developing a staff responsible for campus system security planning, the National Information Assurance Training and Education Center (NIATEC) provides teaching material for use by colleges in reviewing concepts and components necessary for developing an information security plan [11].

The National Institute of Standards and Technology (NIST) Special Publication SP800-30 provides a starting point for planning any information security plan. This publication outlines the steps for conducting a system wide risk analysis [12].

- Step 1 - System Characterization
- Step 2 - Threat Identification
- Step 3 - Vulnerability Identification
- Step 4 - Control Analysis

- Step 5 - Likelihood Determination
- Step 6 - Impact Analysis
- Step 7 - Risk Determination
- Step 8 - Control Recommendations
- Step 9 - Results Documentation

Another NIST document, Information Security Handbook: A Guide for Managers (NIST SP800-100), emphasizes the role of risk management in the information systems security planning process.

II. Results

Information Security Plans, found via the Internet, from 14 universities (Figure 1) were analyzed for commonality and content amongst each other. Most of the individual university security plans cited compliance with FISMA (Gramm-Leach-Bliley Act (GLBA)) as being the cornerstone of their policy. Appendix A, Table 2 shows the results of the comparison. The GLBA mandates that universities appoint an Information Security Plan Coordinator, conduct risk assessments for security and privacy risks, initiate training program for all employees who have access to sheltered data and information, supervise service providers and contracts, and frequently evaluate and adjust their Information Security Programs [13].

Occidental College†
Swarthmore College†
Tulane University†
Hartwick College†
University of Arizona†
University of California†
Belmont University†
Carnegie Mellon†
Michigan Technical University†
University of Nebraska†
Colorado Community College†
University of Georgia†
University of Minnesota†
Stanford University†

Figure 1
List of College Information Security Plans used in Comparative Analysis.
†See Appendix B for Citation.

III. Findings

The authors found that there is no universally accepted standardized format currently used by universities in developing information security plans.

It appears that the main motivation for colleges and universities to develop computer security plans is to demonstrate that they are in compliance with several federal laws. Those laws are: GLBA, FERPA, and HIPPA. In some cases, the university information security plan is actually titled, "Gramm Leach Bliley Act Compliance Plan." Furthermore, the federal agency responsible for ensuring compliance is the FTC. According to Adler, "although the FTC has not begun enforcement actions against higher education institutions, it demonstrated a willingness to pursue noncompliance when it charged three mortgage companies for not following the FTC Safeguards" [14]. The actions of the FTC indicate that higher education institutions may soon become the subject of federal compliance investigations. The FTC provides some general guidance for institutions for building information security plans [15].

Given the focus of this study--college based information security plans--it is not surprising that all the reviewed plans emphasized education and awareness requirements for system users. All the plans appear to have been written with federal law as a motivator. All plans identify an Informant Security Officer. All plans call for periodic review.

While colleges are traditionally thought of as an open information environment, they must also be ever conscious of the dangers in making explicit details of information security plans available on public web sites. Such accessibility might enhance a hacker's ability to do harm to protected systems. Placing too much information on the open Internet about information technology security safeguards, employed on college information systems, creates a possibility for hackers to identify vulnerabilities and weaknesses in college information systems. Avoiding the creation of such vulnerabilities is often referred to as operational security. One definition of operational security is: **"**the process of denying potential adversaries any information about capabilities and/or intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities" [16].

The discovery of the posting of college information system security plans on the Internet raises possible operational security issues. Specifically, systems names, the names and contact information for responsible individuals, and technical information about the composition of the systems may be information best left out of the public domain.

IV. Suggestions

Now that federal agencies have been responding to FISMA, it may be time for college and university system security officers to consider implementing uniform FISMA-like information system security controls. As

cited in the FISMA vision paper, use of a uniform system security planning document can lead to [17]:

- Standards for minimum security requirements for information and information systems;
- Guidance for selecting appropriate security controls for information systems;
- Guidance for assessing security controls in information systems and determining security control effectiveness.

Based on our study of federal guidelines and laws, and a multitude of university plans, the authors propose the use of NIST SP800-18 as the minimum content for university information security plans. (See Appendix A Table 3)

The benefits of having uniform information security plans include:

- A comprehensive guide for use by universities in planning and implementing robust security plans.
- Uniform and consistent reporting by auditors in assuring university compliance to federal information security regulations.
- Clear expression of ownership by senior administration.
- Procedures to be followed when internal abusers of systems are found.

Beyond the format and content of an information security plan, colleges should develop methodology for categorizing the information and the information systems that require protection. Describing systems in a schema which defines the impact of a loss or compromise of those systems or information as being low, moderate, or high can guide a college in designing cost effective security measures. An excellent guide to developing such categorization can be found in NIST Federal Information Processing Standard 199 [18]. Appendix A Table 4 summarizes the FIPS approach impact categorization based upon confidentiality, integrity and availability security objectives.

V. Summary and Recommendations

The authors performed a comparative analysis of 14 college cyber security plans found readily available on the internet. The results of the comparative analysis indicated that there are vast differences in the scope, format and content of college cyber security plans. A review of the literature discovered that the federal government appears to be moving toward a requirement for more uniform college cyber security plan documentation. While most college and university information security plans follow the 5 section format (Gramm Leach Bliley Act (GLBA) Information Security Plan) described by Adler, NIST SP800-18 Appendix A provides a more robust outline for documenting an information security plan [19]. NIST SP800-18 may have greater applicability to a university information security plan. The use of this more extensive reporting methodology will provide college and universities with a deeper understanding of the roles and responsibilities required by all parties in securing that system and subsystems. An outline of those 15 sections is found in Table 3 of Appendix A.

VI. Conclusion

The authors concluded that, while colleges and universities must struggle with the balance between the cost and necessity for information security planning, the need for well-formulated college information security plans is now an integral part of college information technology operations. A study of the implementation of the Federal Information Systems Management Act revealed many similarities between what the federal government is experiencing in securing their systems and how American colleges and universities may benefit from the lessons learned from those experiences. Several guidelines developed by the National Institute of Standards and Technology are extremely helpful in formulating a well thought out and manageable information security plan. One NIST document (FIPS 199) describes distinctions between low, medium and high impact information systems. That guideline also describes recommended security controls appropriate to each of the three levels. The authors believe there is a direct positive correlation between system security planning at the federal level, and similar planning at the college and university level. The apparent movement of the federal government to begin requiring more uniform cyber security planning documentation is an indication that colleges and universities should consider the federal models cited in this article in their respective planning processes.

Colleges and universities will become more likely to be required to submit IT security plans as those institutions begin to interface with U.S. government information systems. We looked at U.S. government guidelines as a known and currently operating set of procedures and policies, because, the government, according to the 2004 National Cyber Security Plan would first attempt to “right itself”, with regards to IT security, then share the results as an example to the private and commercial sectors. Six years have passed since the national plan. In this time, FISMA has been implemented and evaluated. The fulfillment of the federal government mandate requiring IT security plans for any and all organizations whose systems come in contact with government systems is now underway. U.S. colleges will be at the top of the

implementation list given the interaction of colleges with government in areas such as privacy and research.

VII. References

[1] Pappas, Ken. As found in Dolan, Thomas G. Cyber Security. *School Planning and Management.* Retrieved October 4, 2009, from: http://www2.peterli.com/spm/resources/articles/archive.php?article_id=1698.

[2] Internet Crime Complaint Center (IC3), Department of Justice, National White Collar Crime Center. (2009) *2008 Internet Crime Report.* Retrieved November 19, 2009, from: http://www.nw3c.org/downloads/2008_IC3_Annual%20Report_3_27_09_small.pdf

[3] United States Congress. (1999). *Gramm-Leach-Bliley Act.* Retrieved October 4, 2009, from: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ102.106

[4] United States Congress. (1974). *The Family Educational Rights and Privacy Act*. Retrieved October 4, 2009, from: http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

[5] United States Congress. (1996). *Health Insurance Portability and Accountability Act.* Retrieved October 4, 2009. http://www.hhs.gov/ocr/hipaa/.

[6] Gorman, Siobhan. (2009, October 22). China Expands Cyberspying in U.S., Report Says. *Wall Street Journal.* A9.

[7] National Institute for Standards and Technology. (2007). *Information Security Handbook: A Guide for Managers. (*NIST SP800-100). p. 72.

[8] United States Congress. (2002). *Federal Information Security Management Act.* Retrieved October 4, 2009, from: http://csrc.nist.gov/groups/SMA/fisma/index.html.

[9] National Institute for Standards and Technology. (2006). *Guide for Developing Security Plans for Federal Information Systems. (*NIST SP800-18). p. vii.

[10] Microsoft Corporation. (2009). *Developing a Network Security Plan.* Retrieved October 4, 2009, from: http://technet.microsoft.com/en-us/library/cc960627.aspx

[11] National Information Assurance Training and Education Center. (2009). *Pages.* Retrieved October 4, 2009, from: http://niatec.info/pages.aspx.

[12] National Institute for Standards and Technology. (2002). *Risk Management Guide for Information Technology Systems.* (NIST SP800-30). p. 8.

[13] TULANE UNIVERSITY. (2009). *TULANE UNIVERSITY INFORMATION SECURITY PLAN.* Retrieved October 4, 2009, from: http://tulane.edu/tulane/administration/policies/privacy/plan.cfm

[14] Adler, Peter M. (2006) *A Unified Approach to Information Security Compliance*. Retrieved November 10, 2009, from: http://www.educause.edu/EDUCAUSE+Review/EDUCAUSEReviewMagazineVolume41/AUnifiedApproachtoInformationS/158087.

[15] Federal Trade Commission. (2009). *PROTECTING PERSONAL INFORMATION*
A Guide for Business. Retrieved November 10, 2009, from: http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus58.shtm.

[16] National Security Agency, Central Security Service. (2009). *Frequently Asked Questions Terms and Acronyms.* Retrieved November 10, 2009, from: http://www.nsa.gov/about/faqs/terms_acronyms.shtml.

[17] National Institute for Standards and Technology. (2009). *FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) IMPLEMENTATION PROJECT.* Retrieved November 10, 2009, from: http://csrc.nist.gov/groups/SMA/fisma/index.html.

[18] National Institute of Standards and Technology. (2004). *Standards for Security Categorization of Federal Information and Information Systems. (FIPS PUB 199). p.10.*

[19] National Institute for Standards and Technology. (2006). *Guide for Developing Security Plans for Federal Information Systems. (*NIST SP800-18). p. 28.

Appendix A

Table 1: Decomposition of Large and Complex Information Systems.

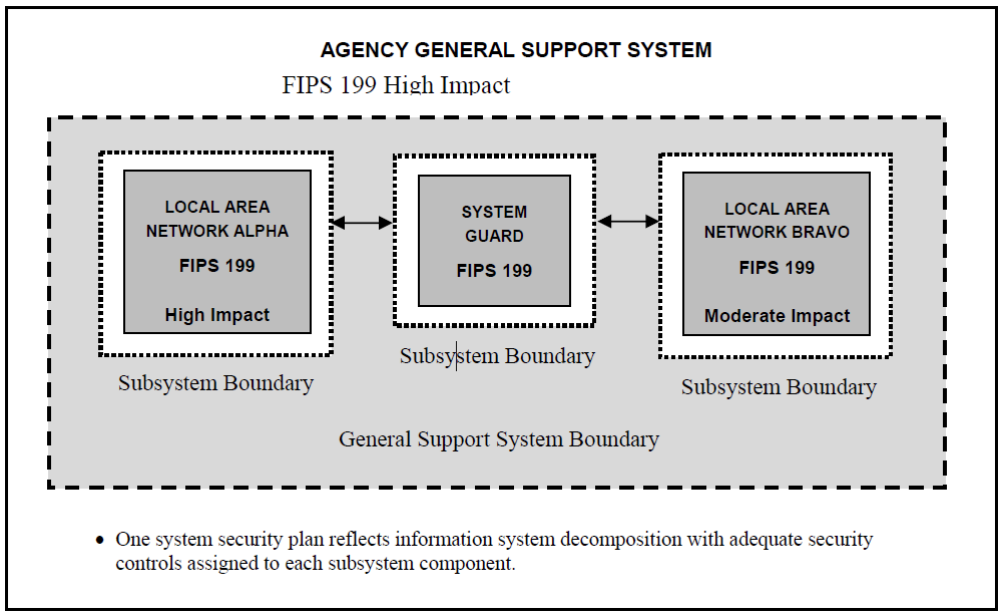

Table 2: Comparison of Chapters in Information security Plans Amongst 14 Colleges.

Colleges (in random order)	GLBA Compliance*	FERPA Compliance*	HIPPA Compliance*	Designation of ISO	Risk Assessment	Training & Awareness	Service Provider & Contractor Guidelines	Continued Evaluation and Revision of Security Plan	Implementation of Safeguards (Physical & Technical)	Employee Background Checks	Confidentiality Agreements	Date Created/Revised	Definitions
College 1	X	X	X	X	X	X	X	X	X				X
College 2	X	X	X	X		X	X	X	X			X	X
College 3	X	X		X	X	X	X	X	X				X
College 4	X	X		X	X	X	X	X	X	X	X		X
College 5	X			X	X	X	X	X	X				
College 6	X	X	X	X	X	X	X	X	X	X	X		X
College 7	X	X		X	X	X	X	X	X	X	X		X
College 8	X	X		X	X	X	X	X	X				
College 9	X			X	X	X	X	X	X				
College 10	X			X	X	X	X	X	X			X	X
College 11	X			X	X	X	X	X	X				
College 12	X	X	X	X	X	X	X	X	X				X
College 13	X			X	X	X	X	X	X			X	X
College 14	X			X	X	X	X	X	X	X		X	

*Cited as the reason security plan was written

TABLE 3: NIST SP800-18 INFORMATION SYSTEM SECURITY PLAN TEMPLATE.

1. Information System Name/Title	**Unique identifier and name given to the system.**
2. Information System Categorization	**Identify the appropriate FIPS 199 categorization.**
3. Information System Owner	**Name, title, agency, address, email address, and phone number of person who owns the system.**
4. Authorizing Official	**Name, title, agency, address, email address, and phone number of the senior management official designated as the authorizing official.**
5. Other Designated Contacts	**List other key personnel, if applicable; include their title, address, email address, and phone number.**
6. Assignment of Security Responsibility	**Name, title, address, email address, and phone number of person who is responsible for the security of the system.**
7. Information System Operational Status	**Indicate the operational status of the system. If more than one status is selected, list which part of the system is covered under each status.**
8. Information System Type	**Indicate if the system is a major application or a general support system. If the system contains minor applications, list them in Section 9. General System Description/Purpose.**

9. General System Description/Purpose	**Describe the function or purpose of the system and the information processes.**
10. System Environment	**Provide a general description of the technical system. Include the primary hardware, software, and communications equipment.**
11. System Interconnections/Information Sharing	**List interconnected systems and system identifiers (if appropriate), provide the system, name, organization, system type (major application or general support system), indicate if there is an ISA/MOU/MOA on file, date of agreement to interconnect, FIPS 199 category, C&A status, and the name of the authorizing official.**
12. Related Laws/Regulations/Policies	**List any laws or regulations that establish specific requirements for the confidentiality, integrity, or availability of the data in the system.**
13. Minimum Security Controls	**Select the appropriate minimum security control baseline (low-, moderate-, high-impact) from NIST SP 800-53, then provide a thorough description of how all the minimum security controls in the applicable baseline are being implemented or planned to be implemented. The description should contain: 1) the security control title; 2) how the security control is being implemented or planned to be implemented; 3) any scoping guidance that has been applied and what type of consideration; and 4) indicate if the security control is a common control and who is**

	responsible for its implementation.
14. Information System Security Plan Completion Date	**Enter the completion date of the plan.**
15. Information System Security Plan Approval Date	**Enter the date the system security plan was approved and indicate if the approval documentation is attached or on file.**

Table 4: NIST Federal Information Processing Standard 199 - POTENTIAL IMPACT DEFINITIONS FOR SECURITY OBJECTIVES

	POTENTIAL IMPACT		
Security Objective	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Appendix B

College and University Information Security Plan Citations

Occidental College	http://www.oxy.edu/x7552.xml
Swarthmore College	http://www.swarthmore.edu/Documents/administration/InfoSecurityPlan.pdf
Tulane University	http://tulane.edu/tulane/administration/policies/privacy/plan.cfm
Hartwick College	http://www.hartwick.edu/x285.xml
University of Arizona	http://www.asu.edu/privacy/security.html
University of California	http://www.ucop.edu/irc/itsec/glbplan/documents/glb_complan.pdf
Belmont University	http://belmont.edu/its/policies/informationsecurity/informationsecurityplan.html
Carnegie Mellon	http://www.cmu.edu/policies/documents/ISP.htm
Michigan Technical University	http://www.admin.mtu.edu/acct/dept/controller/glba/DRAFTappA.pdf
University of Nebraska	http://nebraska.edu/docs/president/26%20Information%20Security%20Plan%20(GLB%20Compliance).pdf
Colorado Community College	http://www.cncc.edu/institutional_research/cccs_it_security_plan.htm
University of Georgia	http://www.uga.edu/audit/glba/policy.html
University of Minnesota	http://www.nacubo.org/documents/business_topics/model_03.doc
Stanford University	http://www.stanford.edu/dept/legal/Worddocs/financialSecurityPlan0903.pdf