# HIGHER EDUCATION AND THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT (2002): A DECADE LATER AND THE CHALLENGES REMAIN

A Capstone Project

By

ALFRED S. BARKER

To

DR. RAY KLUMP

(INFORMATION SECURITY PRACTICUM)

68-595K-SP12

MASTER OF SCIENCE
in
INFORMATION SECURITY

LEWIS UNIVERSITY

April 16, 2012

**ABSTRACT**

The focus of this paper is to highlight and identify key objectives and processes as it applies to higher education and its institutional systems for information and information system security as it relates to the *Federal Information Security Management Act of 2002 (FISMA).* The question is not how the federal government has altered or restricted higher education's ability to provide an open exchange of ideas but one of how has higher education's "academic freedom" based open access model potentially weakened or introduced vulnerabilities and thus risks into an otherwise regulated and secured federal environment of information and information systems. This paper seeks to present an overview of higher education and its potential impact on the *Federal Information Security Management Act* and vise versa, which ultimately demands a structural, social, and legal response to the challenges faced for effectively securing information and information systems. Some of the challenges addressed are attitudes of compliance, cost of compliance and liabilities faced for non-compliance, such as negligence. Key components of *Federal Information Security Management Act* and associated standards are explained with commentary regarding the impact on higher education. At a summary level, higher education and government goals and objectives are compared and contrasted and as applicable demonstrate where complementation exist between both entities. It is hoped that this paper will stimulate more dialogue regarding higher education's need and application of governmental regulatory compliance within context to help effectively safeguard the private and privileged information with which higher education has been entrusted.

**TABLE OF CONTENTS**

**TABLE OF TABLES**

**TABLE OF FIGURES**

## 1. INTRODUCTION

In 2003, the EDUCAUSE Center for Applied Research (ECAR) culminated a year of research with the publication of *Information Technology Security: Governance, Strategy, and Practice in Higher Education* by Robert B. Kavik and John Voloudakis. That study chronicled, "the end of an era in which interpersonal and institutional trust and the academic penchant for openness guided information technology (IT) security strategy at many college and university campuses." [***1***]

> *Since 2006, IT security has continued to rise in importance in higher education, a rise that is reflected in the development of widespread campus IT security programs and national programs sponsored by federal and state governments as well as the development of programs by professional associations. [**1**]*

The relationship between higher education and the *Federal Information Security Management Act* can be challenging. The tension to provide academic information technology systems for faculty, staff and student use with open accessibility, versus the need for operational, business-oriented enterprise systems where "legal compliance, data confidentiality, and security are paramount" has become a fiduciary responsibility. [***2***] Supporting this view are authors Salomon, Cassat, & Thibeau, who attempt to contextualize this attitude and associated challenges by stating,

> *Unlike private corporate networks, which, by their nature, are designed to be "walled gardens" of information, campus networks – due to the need to facilitate collaboration and provide access to information – generally are designed to be more open, and therefore more vulnerable to misuse. [**3**]*

This is even more important now that the federal government has stepped up its efforts to improve and place requirements on various organizations that will exchange information with

other government systems. Higher education is one of these agencies. However, the conditions required for the exchange of information by the federal government with higher education have yet to be acknowledged. In fact, Rodney Peterson and Jack Suess on behalf of the EDUCAUSE/Internet2 Security Task Force attended a briefing of the CSIS[1] Commission on Cyber Security for the 44th President where they expressed their concern that the government has inappropriately categorized higher education as a "government facility" and explained that "we must recognize the higher education sector as a 'critical asset' or 'key resource' in protecting our nation's cyberspace." [***4***]

Three options for higher education's response exists, from holding back and attempting to avoid the evitable, to perhaps a more proactive middle of the road approach by embracing the strengths the new requirements will offer, or going further by contributing to the development process for these standards – as requested by Peterson in his brief. Christopher Jones demonstrates one example of this middle-of-the-road attitude and approach in the following:

> *[T]he implications of having sensitive information compromised are enough to motivate any IT manager to take a closer look at security…; Congress has taken additional steps in the form of regulatory legislation to make certain that every organization covers its bases. Of particular interest to the government sector is the Federal Information Security Management Act of 2002 (FISMA) and a series of documents from the National Institute of Standards and Technology (NIST). Also of great interest and usefulness, the Control Objectives for Information and Related Technology (COBIT)[2] guidelines and recommendations are being used by much of the corporate world to implement*

[1] Center for Strategic & International Studies – http://csis.org/
[2] http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

> *compliance with the Sarbanes-Oxley Act of 2002 (SOX).*[3] *The measures taken to comply with the requirements and recommendations of FISMA, NIST, COBIT, and SOX are equally beneficial to educational institutions.* [***5***]

Much materials referenced may be more commonly understood due to the media's coverage of various corporate entities' debacles (e.g., ENRON) in the private financial corporate sector and the government's response with the implementation of SOX. However, where is the relevance with FISMA? Jones continues by stating,

> *The purpose of FISMA is to provide a comprehensive framework for ensuring the effectiveness and compliance of information security controls. FISMA allows for the development, implementation, and compliance of policies, principles, standards, and guidelines on information security requirements. [**5**]*

Jones expresses the urgency and significance of compliance by stating, "The FISMA and NIST findings and warnings highlight the security risks we now face. Failure to acknowledge security exposures could result in compromised data, compromised system integrity, and the potential for criminal liability." [***5***]

To further a foundational understanding of the relationship between higher education and FISMA, one must define what FISMA is and then explore how this federal statute applies to higher education. Once established, one may shift one's focus from FISMA to higher education's point-of-view to become familiar with how academia fits into the model of regulatory requirements and the challenges this presents.

[3] http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/content-detail.html

***The Demographics of Higher Education***

Higher education is a complex and discrete sector of the economy that share many characteristics and goals, yet varies in size and mission. Comprising of more than 11,000 post-secondary institutions, over 4000 of these are accredited degree-granting colleges serving over 14.5 million students and employing over 3 million faculty and staff within both public and private institutions.

> *"The public verses private distinction is significant… Public colleges and universities rely considerably on funds from state governments… [And] many are considered agencies of state government and are subject to various regulatory and political considerations." [**6**]*

Many states have established "systems" of collectively governed institutions into a single entity with one governing "board." Others have adopted very different models, thus illustrating the varied environment does not suit a single one-size-fits-all solution.

***The Role of FISMA and Higher Education***

Congress passed the *Federal Information Security Management Act (FISMA*) as *Title III of the E-Government Act* (Public Law 107-347) in December 2002 (H.R. 2458-48, SEC. 301). The intent of the regulatory requirement is to ensure that the United States' critical information infrastructure is secure and resilient. FISMA's vision is to promote the development of key security standards and guidelines followed by a practical implementation of procedures for compliance with directives from the National Institute for Standards and Technology (NIST). State governments have begun to embrace these models and are beginning to see the importance of these regulatory statues. "Governors across the country are issuing Executive Orders for strengthening state information technology security, along the lines of the federal government."

[***7***] For instance, on March 19, 2008, the governor of Georgia signed an executive order designed to protect the state's data. The order in part says, "The National Institute of Standards and Technologies has provided a model for information technology security in its implementation of the *Federal Information Security Management Act (FISMA) of 2002*." [***8***] The order continues by establishing authority in stating, "The Georgia Technology Authority's [GTA] [4] office of Information Security is developing technical security standards for use by all [state] agencies that are consistent with the information security risk management model produced by NIST in support of FISMA." [***8***] Each agency within the state is responsible for reporting to GTA at the end of each fiscal year.

> *"In fact, some requirements in NIST publications make system owners accountable to the information security practices of third parties involved in handling agency data. This has resulted in a "trickle down" effect, as state, regional, local and tribal entities, as well as private contractors, realize the importance of being able to express assurance in a way that is acceptable and communicable to their partnering agencies." [**7**]*

Mark Reardon of the Georgia Technology Authority in an article titled *Georgia is on the Right Track with Security as Well* states, "For the first time, agencies will produce uniform ISR's [Information Security Reports] that will allow senior state leaders and citizens alike to measure the effectiveness of the state's information security efforts." Reardon continues by saying, "Many of Georgia's agencies use federal information, and those agencies must use the FISMA risk management framework." [***9***] The University System of Georgia (USG) [5] is a state agency subject to this executive order.

[4] http://gta.georgia.gov/
[5] http://www.usg.edu/

Peter Adler, former Chief Information Security Officer (CISO) of the University of Colorado, in his paper titled *A Uniformed Approach to Information Security Compliance* comments,

> *"Laws and regulations… rarely specify measures that colleges and universities should implement… Yet, a close review of newer statues, regulations, and cases demonstrates that this emerging legal standard for information security closely resembles other established information security standards." [**10**]*

John Voloudakis realizing the implications of the federal law's influence on higher education states, "Given this possibility, it may make sense for Higher Education institutions to become familiar with the standards that FISMA requires and to consider using these as a guide when developing their own information security programs." [***11***]

Adler highlights the need for a more effective unifying approach to information security with a series of steps that parallel FISMA requirements. Paraphrased, these steps are:

1) Organization asset identification and assessment;
2) Conduct regular risk assessment and analysis of results;
3) Safeguards implementation to mitigate identified risk;
4) Address third-party security through constraints or service provider agreements;
5) Include security training as a key part of the program;
6) Monitor and test systems and associated security; and
7) Review and revise the information security program.

Ironically, all of these characteristics are identifiable in FISMA with clear directives and guidance for implementation and application of an effective information security program.

Adler's rewriting of FISMA is most evident when compared to the following bulleted paraphrased information outlined in *H.R. 2458-48, SEC. 301*.[6]

- Risk Assessments – perform periodic assessments of risk and harm to the assets in support of the operations of the agency
- Policies and Procedures – identifying the administrative measures to mitigate and uncover risk throughout the life cycle of information or information systems
- Security Plans – plan for specific system security measures relating to high risk areas previously identified
- Security Awareness Training – annual training provided to personnel, contractors, and all other users accessing the protected systems
- Security Testing and Evaluation – annual testing at a minimum and evaluation of security policies, procedures and operational controls to mitigate risk
- Remediation Procedures – tracking of all security deficiencies identified through testing, monitoring, and a process to measure remediation progress and effectiveness
- Incident Handling and Reporting – establish procedures in accordance with §3546 of *Title III – Information Security* to mitigate, notify, and consult in the event of a breach
- Contingency Plans – produce documented plans with procedures to ensure vital information system continuity of operations should failure or corruption occur.

One can see that the FISMA framework is as complete as Adler's suggestions and has a library of additional supporting special publications and standards. [***12***]

[6] http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

With the relationship between higher education and FISMA established, understanding the existing challenges to comply with this regulatory requirement is needed to complete the foundational introduction.

### *The Challenges of Regulatory Compliance*

FISMA further states that these requirements for compliance include those services or resources "provided or managed by another agency, contractor, or other source (H.R. 2458-51, section 3544, paragraph (a) (1) (A) (ii)". [***13***] This last statement is the challenge public and private higher education must address. Does academia fall into the later categories of "another agency" or "other sources?" What would be the impact, if the higher education were required to bring their information technology systems into compliance with FISMA standards? This challenge is even more evident if one evaluates the measured efforts of various federal agencies demonstrated attempts to bring their organizations into compliance subsequent to FISMA's adoption as law.

Since FISMA's enactment in 2002, it is evident that the federal government's agencies attempts to align themselves with these standards in 2008 have ranked an overall grade average of C-. [***14***] Early in the process, the Office of Management and Budget published an annual "Report Card" expressing the "grade" agencies received after the annual reports were submitted. Unfortunately, however these results were no surprise. For most educational institutions, a C- average would warrant the implementation of an academic probation status. In academia, the typical pervasive attitude is an open and free exchange of information made often with little consideration of the associated risks. Would the results be the same or perhaps worse, if the same FISMA standards were applied today to the higher education information technology systems? Quickly it becomes evident that a significant improvement has not occurred if one evaluates the

results of the grades from the May 2008 release of *Report Card on Computer Security at Federal Departments and Agencies* against previous "report cards," even when considering some of the methodology issues for measuring results. [***15***] Table 1 illustrates the "grades" given, beginning in 2002 when the Act was ratified into law until the presidentially ordered change ending in 2007, to include the annual average "Government-Wide Grade." [***16***]

***Table 1. Federal Computer Security Report Cards: 2002 - 2007***

| **FEDERAL COMPUTER SECURITY REPORT CARDS** | | | | | | |
|---|---|---|---|---|---|---|
| ***Agency*** | ***2002*** | ***2003*** | ***2004*** | ***2005*** | ***2006*** | ***2007*** |
| Agency for International Development | F | C- | A+ | A+ | A+ | A+ |
| Department of Agriculture | F | F | F | F | F | F |
| Department of Commerce | D+ | C- | F | D+ | F | D+ |
| Department of Defense | F | D | D | F | F | D- |
| Department of Education | D | C+ | C | C- | F | C- |
| Department of Energy | F | F | F | F | C- | B+ |
| Department of Health and Human Services | D- | F | F | F | B | B |
| Department of Homeland Security | N/A | F | F | F | D | B+ |
| Department of Justice | Unknown | F | B- | D | A | A+ |
| Department of Labor | C+ | B | B- | A+ | B- | D |
| Department of State | F | F | D+ | F | F | C |
| Department of the Interior | F | F | C+ | F | F | F |
| Department of Transportation | F | D+ | A- | C- | B | D |
| Department of Treasury | F | D | D+ | D- | F | F |
| Department of Veterans Affairs | F | C | F | F | ** | F |
| Environmental Protection Agency | D- | C | B | A+ | A- | A+ |
| General Services Administration | D | D | C+ | A- | A | B+ |
| Housing and Urban Development | F | F | F | D+ | A+ | A |

| | | | | | | |
|---|---|---|---|---|---|---|
| National Aeronautics and Space Administration | D+ | D- | D- | B- | D- | C |
| National Science Foundation | D- | A- | C+ | A | A+ | A+ |
| Nuclear Regulatory Commission | C | A | B+ | D | F | F |
| Office of Personnel Management | F | D- | C- | A+ | A+ | A- |
| Small Business Administration | F | C- | D- | C+ | B+ | B |
| Social Security Administration | B- | B+ | B | A+ | A | A+ |
| ***Government-Wide Grade*** | | **D** | **D+** | **D+** | **C-** | **C** |

**** Did not provide FY06 FISMA Report**

This report-card-based process ended when this model shifted from the paper-driven and much criticized method of reporting to the on-line paper-less version. [***17***]

The current reporting model no longer expresses success as a grade, but more cryptically expresses the report as a percentage of agencies that were prepared. [***18***] In fairness, these previous observations were not to exemplify the shortcomings of various agencies in the federal government. Nor were these observations to suggest that the standards, expectations, or measurable outcomes of FISMA were inappropriate. The examples given in Table 2 were to highlight the challenge for any organization to transition the culture and technological infrastructure to a secure information environment. [***18***] This new reporting model supports this intent. As of the most recent report in *Information Week*, the inspector generals of half of the twenty-four reporting agencies declared that the percentages of compliance has slipped, while only seven agencies reported a 90% compliant program status, "with the National Science Foundation (NSF) topping the list with 98.8% compliance."

> *However, even that was a very slight slip from last year, when the NSF achieved 98.9% FISMA compliance, according to the OMB report…. Other agencies at the top of the list in compliance are the Social Security Administration (96.9%), the Environmental*

> *Protection Agency (94.9%), the Nuclear Regulatory Commission (94.8%), the Department of Homeland Security (DHS) (93.4%), NASA (92.9%), and the Department of Justice (91.2%). Still, the SSA [Social Security Agency], EPA [Environmental Protection Agency], and NRC [Nuclear Regulatory Commission] all achieved lower compliance scores from last year, when they were 100%, 99.2% and 96.7% compliant, respectively. [**19**]*

***Table 2. Overall Inspector Generals Findings by Information Security Area***

| | Compliant Program | | Needs Improvement | | Program Not Implemented | |
|---|---|---|---|---|---|---|
| ***Cyber Security Program Area*** | ***No.*** | ***%*** | ***No.*** | ***%*** | ***No.*** | ***%*** |
| Security Authorization | 13 | 54 | 11 | 46 | 0 | 0 |
| Configuration Management | 6 | 25 | 18 | 75 | 0 | 0 |
| Incident Response | 15 | 62 | 9 | 38 | 0 | 0 |
| Security Training | 7 | 29 | 17 | 71 | 0 | 0 |
| POA&M[7] | 8 | 33 | 16 | 67 | 0 | 0 |
| Remote Access | 10 | 42 | 14 | 58 | 0 | 0 |
| Account and Identity Management | 5 | 21 | 19 | 79 | 0 | 0 |
| Continuous Monitoring | 7 | 29 | 15 | 63 | 2 | 8 |
| Contingency Planning | 8 | 33 | 16 | 67 | 0 | 0 |
| Contractor Oversight | 6 | 25 | 16 | 67 | 2 | 8 |

Earlier the rhetorical question was asked, "does academia fall into the latter categories of 'another agency' or 'other sources'." This question does have an answer – in two parts. It begins with the January 2011 published report *Cybersecurity Two Years Later,* in response to the briefing Rodney Peterson and Jack Suess attended for the 44th President where they expressed,

[7] Plan of Action & Milestones

"We must recognize the higher education sector as a 'critical asset'." The President heard Peterson's comments and one year later, "On May 29, 2009, the President declared cyberspace as a critical national asset." [***20***] The second part follows rather rapidly in the form of the November 2011 Department of Homeland Security's[8] *Blueprint for a Secure Cyber Future* where DHS classifies higher education as one, a Federal Department (U.S. Department of Education)[9] and as two, a private sector stakeholder, which defined are organizations and entities that are not part of any government structure to include for-profit and not-for-profit organizations – including "academia." [***21***]

As has been established, there is evidence of the application of FISMA at both the federal and state levels, which has influenced how higher education must conduct information security. Also established, cyberspace is now considered a critical national asset and higher education has now been defined as a private sector stakeholder within the context of the federal government. Therefore, the continued purpose of this paper is to explore higher education and FISMA from the perspective of the educational and governmental goals and objectives; the challenges and problems of leadership as it applies to legal liability for failure to comply with regulatory standards; expose real-world examples of possible neglect of due diligence; influences of the possible federal mandates and the attitudes with government alignment and objections; and higher education's challenge with FISMA compliance. To establish the context of the information discussed, a review of the literature follows.

[8] http://www.dhs.gov/index.shtm
[9] http://www.ed.gov/

## 2. EVOLUTION OF COMPLIANCE

Bill Readings' acclaimed scholarly review of the university system's growing loss of identity was used in exploring the pervasive attitudes found within academia. [***22***] Supplementing Readings' view is Lawrence White's 2005 vision into the future *Which Legal Issues Will Keep Colleges Busy in the Year 2012*. [***23***] The databases of ACM [10] were researched; ACM is a highly recognized premier membership organization for computing professionals. The databases of Georgia's GIL Express [11] and GALILEO [12] were also used. Extensively accessed were the databases of *EDUCAUSE Journal* and *EDUCAUSE Quarterly*, as well as the joint ventures of EDUCAUSE and Internet2. EDUCAUSE is "a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology. EDUCAUSE helps those who lead, manage, and use information resources to shape strategic decisions at every level. A comprehensive range of resources and activities is available to all interested employees at EDUCAUSE member organizations, with special opportunities open to designated member representatives." [***24***] The Office's of the White House, the Office of Management and Budget (OMB), and the Office of the Department of Homeland Security (DHS) provided invaluable documentation in support of the progressive information needed to illustrate the status of compliance and the direction the regulatory requirements are heading. Since FISMA's introduction, a decade has passed and the scope of the materials referenced is reflected. There has been quite an evolution in compliance from a costly paper-based system to a streamlined digital format. As the National Institute of Standards and Technology is the repository of FISMA documentation, introducing NIST, the importance of FIPS and the process of vetting are most important to the overall comprehension of the topic.

[10] Association for Computing Machines – http://www.acm.org/
[11] Georgia Interconnected Libraries – http://gil.usg.edu/gilhome/about/page/category/about_gilfind
[12] **G**eorgi**A** **L**Ibrary **LE**arning **O**nline – http://gil.usg.edu/gilhome/galileo/page/category/about_galileo/

***National Institute of Standards and Technology***

The *NIST Federal Information Processing Standards* (FIPS 199, FIPS 200) [13] and various guidelines in the 800-series Special Publications [14] characterize the information security standards for application of the FISMA initiative. [***12***] These standards in general apply to non-national security federal information systems. Assigned to NIST are specific responsibilities of development, which include:

- Standards to be used by federal agencies
- Categorize information and information systems
    - Categorization is to be based on predefined objectives e.g., the functional organization's application of the information or information system
    - The category of security provisioning is to be at an appropriate level in accordance with the level of risk for the information or information system
- Guidelines to recommend the various types of information and information systems to be categorized
- Minimum information and information systems security requirements for the management, operational requirements, and technical security controls for each category

***The Importance of FIPS***

The directives in the FIPS guidelines and 800-series special publications are beneficial regardless of the need for regulatory compliance. Dr. Ron Ross from the Computer Security Division of NIST stated:

> *Through some of the legislative policy drivers, such as the Federal Information Security Management Act (FISMA), we can build a solid foundation of information security by*

[13] http://csrc.nist.gov/publications/PubsFIPS.html
[14] http://csrc.nist.gov/publications/PubsSPs.html

> *establishing a fundamental level of "security due diligence." FISMA characteristics were covered in more detail through a risk management framework and information security program. These standards should not drive the mission of an organization, but rather support the mission. The policies and procedures developed from these are a corporate commitment for protecting the critical enterprise.* [***13***]

Likewise, a similar response came from Brian Markham during a 2007 EDUCAUSE Higher Education conference where he stated:

> *As a response to FISMA, NIST developed FIPS-199 in 2003. FIPS-199 is the Federal Government's answer to data classification. It is a framework that can be easily understood, adopted, and implemented. It is based upon two components: security objectives and potential impacts.… Being in line with FIPS-199 can only help us in the federal grant application process. [***25***]*

Ironically, it is oftentimes here during communications about federal grants where higher education and the federal government meet, and FISMA certified and accredited system must exist to support mandated secure communications. [***26***]

***Security Controls***

Security Controls[15] associated with the *FIPS 199* and *FIPS 200* framework results from the effective application of the *NIST Special Publication 800-53 Revision 2*. This publication provides guidelines for selecting and specifying security controls for information systems. The intent of the guidelines is to give practical insight into securing information systems operated by the federal government. Some of the objectives for this publication include:

[15] Security Controls are safeguards or countermeasures to avoid, counteract or minimize security risks.

- Facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems;
- Providing a recommendation for minimum-security controls for information systems categorized in accordance with *FIPS 199, Standards for Security Categorization of Federal Information and Information Systems*; [***12***]
- Providing a stable, yet flexible catalog of security controls for information systems to meet current organizational protection needs and the demands of future protection needs based on changing requirements and technologies; and
- Creating a foundation for the development of assessment methods and procedures for measuring security control effectiveness. [***27***]

These technically written publications are guidelines and complement other guidelines written in support of non-national security systems. When these guidelines were constructed, consideration was given to not only include agencies of the federal government, but other institutions such as state, local, and tribal governments, and private sector organizations to encourage their use of these guidelines, as appropriate. The security controls identified in *Special Publication 800-53* encompass the following subjects:

- Risk Assessment
- Certification, Accreditation and Security Assessments
- System Services and Acquisition
- Security Planning
- Configuration Management
- System and Communications Protection
- Personnel Security

- Awareness and Training
- Physical and Environmental Protection
- Media Protection
- Contingency Planning
- Maintenance
- System and Information Integrity
- Incident Response
- Identification and Authentication
- Access Control
- Accountability and Audit [***28***]

***Public Review Process***

To support this framework, NIST employs a comprehensive public review process for every FISMA standard and guideline to ensure the security standards and guidelines undergo a peer review process that is technical, and to evaluate implementation challenges. A paraphrase of those particulars includes:

- Solicitation of feedback from individuals and organizations in the public and private sectors to provide insight on the content and application of each of the FISMA publications
- Security publications incur three full public vetting cycles to provide individuals and organizations an opportunity to actively participate in the development of the standards and guidelines
- Work closely with owners, operators, and administrators of information systems within the NIST organization to obtain real-time feedback on the challenges associated with the

implementation of specific safeguards and countermeasures (i.e., security controls) being proposed for federal information systems

- NIST has an extensive outreach program that maintains close contact with security professionals at all levels to incorporate important feedback into future updates of the security standards and guidelines.

This process of public outreach program and review process for standards and guideline development, along with prototyping and implementing safeguards and countermeasures in the information systems owned and operated by NIST, presents a complete security lifecycle in support of its constituents. These processes produce high quality, well-accepted security standards and guidelines that are in use by the federal government, and embraced by many organizations in the private sector. [***29***] For higher education, there is little risk in embracing these standards; more so, higher education's position in society is to join their efforts, contribute, and influence the processes to support information systems security.

## 3. GOALS AND OBJECTIVES

"Technology has a significant impact on our economy and on society in general. As a result, Congress, state legislatures, and an expanding variety of government agencies – internationally and domestically – are creating technology-related laws and regulations. In some cases, the affect on colleges and universities is direct and targeted; in others, it is indirect or even accidental. Regardless, complying with such requirements remains a moving target that often requires knowledge-sharing and collaboration among multiple institutions." [***30***] This introduces challenges for leadership within higher education. Of these challenges, this section will address establishing perspective – learning what the federal government expects, and understanding the FISMA framework and the implementation process. Also explored is the need to understand the secure communications and identity and access management (IAM) program implemented by OMB to enhance the abilities of federal agencies and stakeholders to securely report digitally. Lastly, the regulatory landscape is discussed with the focus on seeking a balance between the needs of higher education and those of the federal government.

### *The Challenges of Leadership*

One of the goals and objectives of FISMA is to bring technological security relevance to senior leadership decision-making process.

> *FISMA specifically addresses senior management responsibility, not technical specifications. Technical solutions alone will not be sufficient for agencies to earn good marks on FISMA compliance. Rather, agencies must demonstrate how information security technology fits into the framework of an overall security strategy and budget that is in turn integrated with each agency's mission and goals. FISMA compliance therefore requires not only new initiatives, but also a new perspective from the head of the agency*

> *down to the security administrator…. In complying with FISMA, therefore, agency heads must not only become familiar with security risk management, they must also take an active role in the oversight of information security policies and practices in their agency, as well as prepare required reports mandated by FISMA. [***13***]*

Similarly, leadership in higher education institutions regarding their information and information systems must be aware of the risk the open and liberal access ethos – spoken of earlier – has, and attempt to balance priorities and functionality. Addressing information security risk requires continued investment by leadership because there is no one solution that addresses all the requirements.

> *Protecting information assets implies that we need to identify what is really at stake. Securing the growing proliferation of data communication in practically every aspect of an enterprise is one of the major challenges that every manager and administrator faces today.* [***2***]

The American Council for Technology and Industry Advisory Council, in a paper titled *Business Value of CFO-CIO Collaboration,* identified some of the business benefits of senior executive leadership for the Chief Financial Officer (CFO) and the Chief Information Officer (CIO) collaboration. The guidance they issued reads; "Both CFO and CIO should strive to understand the other's areas of responsibility and expertise where overlapping responsibilities should be viewed as a shared interest." [***31***] This need for collaboration has become a key issue for every executive, whether in the government or private sector stakeholders. One executive focuses on maintaining and demonstrating fiscal responsibility, while the other applies information technology within the constraints of operational business functions and budgetary constraints. The results of their survey from the aforementioned paper also concluded that

interdependence is crucial to the success of the organization. "In meeting legislative and regulatory requirements we find that CFOs and CIOs work together to meet milestones and identify requirements to input into the budget. They work together to present a united front and hold the functional teams accountable for the results." [***31***]

A few of the lessons learned from their research follows:

- *Each executive organization has core competencies and defined roles necessary for program success. These included:*
    - *CIO responsibility for telecommunications, infrastructure, and information security…*
- *Early collaboration identifies issues and helps to mitigate program risk…*
- *Open dialog enables stakeholder consensus and program success...*
- *Common business goals and objectives must be identified and accepted by all parties involved.*
- *Maximize the representation of the programs in planning to bring the necessary business needs and technical expertise into the decision making process…*
- *Include the CIO early in the planning process... Early CIO representation is critical to understanding IT constraints and goals so the review can move forward with a focus on business value and the customer(s)….*

*Ultimately, the number one lesson learned from this work on collaboration is in creating an environment that promotes effective communication…. allows both CFO and CIO to contribute their experiences, knowledge, and understanding to achievement…. The result is a more cooperative environment that serves as a model for leadership and demonstrates effective program/project management. [***31***]*

However, the introduction of "C" level managerial positions to meet FISMA objectives has affected higher education. Rodney Petersen in *Safeguarding the Assets in Higher Education – The role of the CSO* [16], comments on the cultural distinctions of the CIO and CISO role within the higher educational context. An example, CIOs and CISOs are a relatively new phenomenon within higher education. As a result, many information technologist whose responsibilities were network administration now find that information security responsibilities are appended as the "and other duties assigned" clause to his or her job description, which has caused issues in establishing accountability. In some instances, the CISO is a member of the institution's executive council. Whereas in other institutions, the CISO reports to the CFO within the context of a business function – such as auditing or legal. Yet, other institutions have the CISO reporting to the CIO within the context of information technology. Kathy Bergsma of EDUCAUSE and Internet2 adds,

> *The vast majority of those in an ISO/CISO position [within higher education] held previous positions in IT and came from higher education backgrounds. Institutions appear to be recruiting security officers from IT managerial ranks. Often these folks started with very strong technical experience and have now developed skills in business process analysis, thus moving away from hands-on activities. [***32***]*

Each model has its strengths, opportunities, and weaknesses and is often a by-product of the culture of each institution. Comparatively, the corporate environment does not suffer these issues. Petersen demonstrates the difference and complementation between government, private sector stakeholders, and the current higher education ethos for information systems leadership. For instance, "There has also been much criticism of the incompatibility between academic

[16] Often the term Chief Security Officer (CSO) and Chief Information Security Officer (CISO) is used interchangeably as seem here.

organizations and the need to develop a "culture of secrecy." Therefore, the process needs are increasingly important for colleges and universities and include such elements as security strategy, policy development and enforcement, physical security, and security program administration." [***33***] Meanwhile, the legislators that constructed the requirements listed in FISMA understood how critical it was for the security of information and information systems that these two executives have comparable influence. Recognized is the need for the task of information security to move beyond the "small cadre" of individuals with technical security training and acknowledge the challenge of ownership is at the highest level of the higher educational institute. [***2***] As identified in FISMA, functionality of the government agency/stakeholders and security risk management ownership is a requirement and not an option for senior leadership. Therefore flowing from the top down, a culture of information security must pervade throughout all aspects of the organization.

One of the most important management tools and a key indicator of a mature information technology security program is the existence of IT security governance.

> *IT security governance is the system by which an organization directs and controls IT security… governance determines who is authorized to make decisions. Governance specifies the accountability framework and provides oversight to ensure that risks are adequately mitigated. [***32***]*

Kathy Bergsma described governance in her paper *Information Security Governance* as the assurance that security strategies of an organization are aligned with the objectives of that organization and remains consistent with regulations. How does one go about establishing early the importance of governance? One must begin with an established mission, vision, and shared values statement. This statement drives the creation of a *Strategic Plan,* which in turn

establishes actionable objectives. It is these objectives that policy is written around and on policy Bergsma writes,

> *Information security policy is an aggregate of directives, rules, and practices that prescribes how an organization manages, protects, and distributes information. Information security policy is an essential component of information security governance---without the policy, governance has no substance and rules to enforce. Information security policy should be based on a combination of appropriate legislation, such as FISMA; applicable standards, such as NIST Federal Information Processing Standards (FIPS) and guidance; and internal agency requirements…. IT and data within higher education information systems are becoming increasingly regulated and scrutinized. This regulation ranges from pressures for disclosure and transparency to pressures for privacy. These pressures accent the need for common approaches, common solutions, and consistent high-quality data.*

In order to identify the challenges in conjunction with the keys needed to succeed against the pressures mentioned, Bergsma adds one needs to be proficient in:

- *Balancing extensive requirement originating from multiple governing bodies;*
- *Balancing legislation and agency specific policy;*
- *Maintain currency; and*
- *Prioritizing available funding according to requirements. [**32**]*

Bergsma summarizes by stating, "Higher education information systems continue to be subject to a large number of security threats. The ability to secure the gamut of intuitional IT resources and data has become a compelling and increasingly urgent need." [***32***]

***Establishing Perspective***

FISMA explicitly emphasizes a risk-based policy for cost-effective security. In support of and reinforcing this legislation, the Office of Management and Budget (OMB) in *Circular A-130, Appendix III, Security of Federal Automated Information Resources*, requires executive agencies within the federal government to comply and ensure that these processes are effectively being implemented:

- Plan for security;
- Ensure that appropriate officials are assigned security responsibility;
- Periodically review the security controls in their information systems; and
- Authorize system processing prior to operations and, periodically, thereafter. [***34***]

These responsibilities for management presume that designated agency officials understand the risks and other factors that could adversely affect their missions. Moreover, these officials must understand the status of their security programs and the security controls planned or in place to protect their information and information systems in order to make informed judgments and investments that appropriately mitigate risk to an acceptable level. The ultimate objective is to conduct the day-to-day operations of the agency and accomplish the agency's stated missions with adequate security, or security commensurate with risk, considering the level of harm possible from unauthorized access, use, disclosure, disruption, modification, or destruction of information. To support this requirement, a key element of the FISMA Implementation Project is NIST, which was developed as an integrated risk framework to effectively bring together all of the FISMA-related security standards and guidance to promote the development of comprehensive and balanced information security programs. [***35***]

Management's responsibilities are also included in FISMA to address the *Acquisition and Accreditation Regulatory Requirements for Information Systems.* The Federal Acquisition Regulations (FAR) reference FISMA in their documentation and state,

> *Agency-head responsibilities – The agency head or a designee shall prescribe procedures for ensuring that agency planners on information technology acquisitions comply with the information technology security requirements in the "Federal Information Security Management Act (44 U.S.C. 3544)." [***36***]*

FAR utilizes the FISMA, *OMB Circular A-130*, and the security standards and guidance developed by the National Institute of Standards and Technology at the Department of Commerce. [***36***] This applies to the types of accredited and certified systems that are allowable for use and connectivity to federal systems; more specifically, those systems that remotely connect as an extended end-node. Since most information system interfaces are becoming portal based, or utilizes a secure download or exchange method, this reduces higher education's impact, unless the information system must perform a service or store sensitive or confidential information. Most systems outside of the protected environment utilize a hardened front-end or portal which secures the transportation of information via a certificate-based VPN tunnel or some other means of secure encrypted transportation. The end-node acts as little more than a terminal in that it does not process or store data viewed within the portal. The front-end is a hardened bastion used to access the protected systems on the back-end. Regardless, it will remain a consideration when determining compliance with FISMA regulatory requirements.

### *FISMA's Framework*

As mentioned above, FISMA explicitly emphasizes a risk-based policy for cost-effective security. For this policy to be effective, management must assess and analyze quantitatively or

qualitatively the organizational risks. The Risk Management Framework (Figure 1) is a system designed by NIST in support of FISMA to allow management the ability to perform this task in an organized and directed method allowing for flexibility in the form of six steps, which are:

*Step 1: Categorize*

***Categorize*** *the information system and the information processed, stored, and transmitted by that system based on an impact analysis.*

*Step 2: Select*

***Select*** *an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on organization assessment of risk and local conditions.*

*Step 3: Implement*

***Implement*** *the security controls and document how the controls are deployed within the information system and environment of operation…*

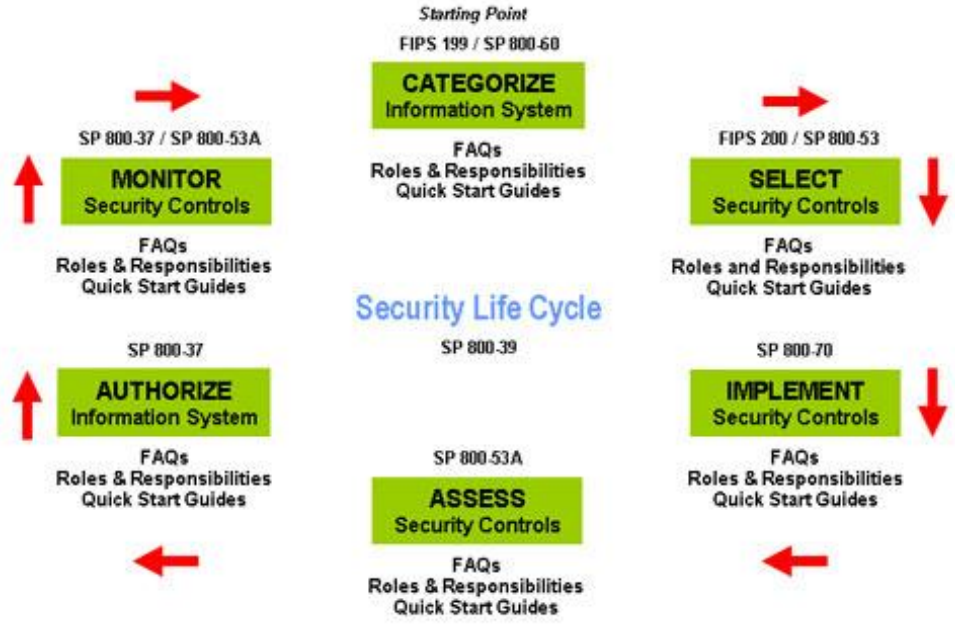


***Figure 1. FISMA Risk Management Framework***

> *Step 4: Assess*
>
> ***Assess*** *the security controls using appropriate procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.*
>
> *Step 5: Authorize*
>
> ***Authorize*** *information system operation based upon a determination of the risk to organizational operations and assets, individuals, other organizations and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.*
>
> *Step 6: Monitor*
>
> ***Monitor*** *and assess selected security controls in the information system on an ongoing basis including assessing security control effectiveness, documenting changes to the system or environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to appropriate organizational officials. [***35***]*

One accomplishes this through the application of the *Federal Information Processing Standards* (FIPS), *Special Publications* (SP's),[17] and *Quick Start Guides* (QSG's).[18] Each step has associated with it a document or series of documents providing the required information and instruction needed to implement the framework. [***37***]

### *Federal Implementation Project*

In January 2003, the FISMA Implementation Project established the aforementioned risk management framework to integrate effectively all of NIST's FISMA-related security standards

[17] Special Publications
[18] Quick Start Guides

and guidelines. The objective of the Risk Management Framework and the associated publications was to support agencies in the day-to-day operations of information or information systems, the agency's functional mission(s), and provide sufficient security proportionate with the associated level of risk. This framework included the avoidance and mitigation of unauthorized access, use, disclosure, disruption, modification, or destruction of information. [***38***] The significance of this project was that the federal government understood that for this FISMA initiative to be effective it would have to implement and promote a project management framework to support the transition of all federal agencies. Similarly, higher education will need to give this framework the same consideration as they come to terms with the appropriate levels of regulatory compliance.

***The Implementation Process***

The FISMA implementation process has several phases of integration clearly defined for federal agencies to assimilate into their operational process. The first phase of the FISMA Implementation Project focuses on the development of the security standards and guidance required to implement effectively the provisions of the legislation. The implementation of the NIST standards and guidance will help agencies create robust information security programs and effectively manage risk to agency operations, agency assets, and individuals. To develop and implement a security program, review all key documentation and the risk management life-cycle process. This risk management life-cycle process is continuous as is the development of new and innovative technologies to support information systems. [***13***] NIST has published the *Development Schedule for FISMA Implementation Project Publications* (Table 3) as of February 21, 2012, which addresses the revised milestones and the recommended documentation.

***Table 3. Development Schedule for FISMA Implementation Project Publications*** [19]

| | | Jan 2012 | Feb 2012 | Mar 2012 | Apr 2012 | May 2012 | Jun 2012 | Jul 2012 | Aug 2012 | Sep 2012 | Oct 2012 | Nov 2012 | Dec 2012 | Jan 2013 | Feb 2013 | Mar 2013 | Apr 2013 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FIPS 199 | Final | | | | | | | | | | | | | | | | |
| FIPS 200 | Final | | | | | | | | | | | | | | | | |
| SP 800-18, Rev 2 | | | | RVC | RVC | RVC | RVC | RVC | 1PD | RVC | FPD | RVC | Final | | | | |
| SP 800-30, Rev 1 *JTF* | | RVC | RVC | RVC | RVC | FPD | RVC | RVC | Final | | | | | | | | |
| SP 800-37, Rev 1 *JTF* | Final | | | | | | | | | | | | | | | | |
| SP 800-39 *JTF* | Final | | | | | | | | | | | | | | | | |
| SP 800-53, Rev 3 *JTF* | Final | | | | | | | | | | | | | | | | |
| SP 800-53, Rev 4 *JTF* | | RVC | IPD | RVC | RVC | RVC | RVC | Final | | | | | | | | | |
| SP 800-53A, Rev 1 *JTF* | Final | | | | | | | | | | | | | | | | |
| SP 800-53A, Rev 2 *JTF* | | | | | | RVC | RVC | RVC | 1PD | RVC | FPD | RVC | Final | | | | |
| SP 800-59 | Final | | | | | | | | | | | | | | | | |
| SP 800-60, Rev 1 | Final | | | | | | | | | | | | | | | | |
| SP 800-137 | Final | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | |

The second phase of the FISMA Implementation Project is to focus on the development of a program for "credentialing" public, private sector stakeholders, and organizations to provide security assessment services for federal agencies and others. The security services involve the comprehensive assessment of the management, operational, and technical security controls in federal information systems including the assessment of the information technology products and services used in security control implementation. The security assessment services will determine the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. To support implementation of the Organizational Credentialing Program and aid security assessments, this phase of the FISMA Implementation Project will also include the initiatives for *Training, Product and Services Assurance Assessment, Support Tools,* and *Harmonization*. All of these, per their title, are self-explanatory with the exception of *Harmonization,* which will focus on synthesizing or mapping other existing industry standards

[19] **LEGEND: 1PD:** Initial public draft; **2PD:** Second public draft; **3PD:** Third public draft; **FPD:** Final public draft; **RVC:** Revision cycle; **JTF:** Joint Task Force Transformation Initiative

such the International Organization for Standardization / International Electro technical Commission (ISO/IEC) 27000:2009 [20] series to NIST 800 series of special publications. [***13***] For example:

> *The objectives of ISO/IEC 27000:2009 are to provide terms and definitions, and an introduction to the ISMS [21] family of standards that:*
>
> 1. *Define requirements for an ISMS and for those certifying such systems;*
> 2. *Provide direct support, detailed guidance and/or interpretation for the overall Plan-Do-Check-Act (PDCA) processes and requirements;*
> 3. *Address sector-specific guidelines for ISMS; and*
> 4. *Address conformity assessment for ISMS. [**39**]*

Organizations could also participate in the credentialing program to demonstrate competence in the application of the NIST security standards and guidelines. Through the development of a network of credentialed organizations with accredited and certified competence in the provision of security assessment services, federal agencies and stakeholders will gain greater confidence in the use of these services. Again, it would seem beneficial for higher education to embrace opportunities to be involved in the process. This would enable higher education to have its needs represented and accredited resources identified, to support the very demanding requirements information and information system assurance and risk management places upon the institution.

It will require thorough consideration and prioritization of controls and resources to implement effectively FISMA compliance. Prioritizing security controls recommended by NIST may place emphasis on selected security controls possibly at the expense of other important controls. The approach presented provides organizations with a regimented, well thought-out,

[20] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41933
[21] Information Security Management System

and adaptable process to select appropriate security controls for their information and information systems. It suggests a methodology to determine the effectiveness of those controls, and a process to monitor residual risks to the organization's operations and assets, individuals, and other organizations. NIST's or comparable standards (harmonized/mapped standards) deployment of security controls use a defense-in-depth approach to combine management, operational, and technical safeguards and countermeasures to address all aspects of the user, service, or physical threat space. This balanced approach to control selection and deployment recognizes that technology alone cannot protect federal or other information systems. What it does identify is a holistic approach needed to protect critical mission and business functions, which includes people, processes, and technology working together in a complementary and mutually reinforcing manner.

***Improving Secure Access***

In 2008, the Department of Homeland Security introduced a shift in the reporting model and its associated identity and access management controls with the issuance of *Homeland Security Presidential Directive 12 (HSPD-12)*. [***40***] Referencing the directive, John Voloudakis comments that HSPD-12 "requires the use of more uniform, secure standards for issuing government identity credentials. The *Federal Information Processing Standards (FIPS) Publication 201-1*… describes standards for the proposed Personal Identity Verification, or PIV, system. HSPD-12 calls for these standards to be implemented both by federal offices and by 'contractors.'" [***11***] If this interpretation of terminology is to include programs funded by federal dollars, "colleges and universities also may have to comply. Institutions considering an identity management solution may want to use this standard as a guide when looking at their own systems." [***11***] With the exception of a very few enclaves, FISMA has not as of yet been

extended to include higher educational institutions as a critically protected system. Voloudakis suggests that the question of compliance boils down to a legal interpretation of the regulatory requirement per a specific context of application. In the case identified above, higher education would have to address how to functionally apply identity and access control management within their university system. EDUCAUSE's 2012 policy statement also supports the identification of IAM as the "most pressing higher education IT challenges that continues to grow in importance as institutions attempt to handle increasingly complex technologies, as well as diverse and challenging access needs… which imposes legal, audit, security, and support challenges." [***30***] Again, these challenges have yet to be formally addressed.

Assuming most institutions are implementing these controls, this statement is just sidestepping the issue. What is the issue? To impose politically a legal constraint upon higher education is not popular for all parties involved. Few ever commit to drawing a direct line of correlation to information or information systems security programs due to the possible political consequence or fallout from the cries of impinging upon academic freedom. So, is there a balance?

### *Regulatory Landscape – Seeking a Balance*

The goal is to explore the current regulatory landscape and the factors contributing to the need for information and information system security standards that comply with FISMA and other similar regulatory requirements. In their 1999 report *Some Assembly Required: Building a Digital Government for the 21st Century*, Dawes, Bloniarz, Kelly, & Fletcher highlight some of the benefits and challenges the government offers to empower any society and the impact on education. A few of these expectations are new models for public-private partnerships and other networked organizational forms, archiving and electronic records management, better methods of

IT management, and matching research resources to government needs. The significance of this focus seems clearly articulated in the content of FISMA's regulatory requirements. FISMA addresses all of the above objectives and the Risk Management Framework earlier outlined directly relates to higher educational needs. [***41***]

In a *VeriSign* white paper, *FISMA: Making the Grade - an Introduction to the Federal Information Security Management Act* infers that the FISMA regulatory requirements are the results of technology development, integration and an inappropriate "open environment" for information exchange that government entities have been practicing for many years.

> *In the late 20th and early 21st centuries, government agencies had rapidly migrated to transformational, Internet-based communication systems. While this migration greatly improved performance and increasingly facilitated tighter coordination among disparate agencies, the resulting highly "open" nature of the current, federal computing environment also presented a new category of risk as threats to federal systems become more varied and sophisticated. [***42***]*

There is a correlation of comparison and resolve to our current higher educational information systems and the "open exchange." Sadowsky, Dempsey, Greenberg, Mack, & Schwartz draw the same conclusion as they expound on a need for balance.

> *Technology is changing so rapidly and new cyber threats are emerging with such swiftness that government regulation can become a straitjacket, impeding the development and deployment of innovative responses. It is important therefore to achieve the right balance of regulatory and non-regulatory measures. [***43***]*

Addressing this concept of balancing higher education's challenge for operational functionality with governmental mandates, authors Sadowsky, et al., continue to elaborate on the particulars of what this "balance" implies.

> *The challenge is to adopt government policies that maximize the benefits of government involvement without stifling innovation through overbearing regulation and technology mandates. Within a framework of partnership, the solution can be found in a balanced approach that includes:*
>
> - *Market forces that encourage private enterprises to address the security of their computer systems in order to protect their profitability;*
> - *The government's research and awareness-building functions;*
> - *Computer crime laws protecting both government and privately owned computers and networks;*
> - *Traditional concepts of legal liability translated to the computer context; and*
> - *Laws, regulations, and government policies that are specifically focused on promoting computer security. [**43**]*

The key point is to promote information security without stifling operational functional productivity. "The challenge for governments is to assure that we can realize the benefits of emerging technologies and still maintain the values and freedoms that we enjoyed without them." [***43***] Can the higher educational system live and operate in both technologically functional worlds?

Higher education must seek to apprehend the significance of the threat technology introduces and integrate an effective methodology to negotiate this challenge. For instance, higher education may be accessible to federal information systems used or operated by an

executive agency or by another organization on behalf of an executive agency through government contracts – agencies such as the Department of Defense, Department of Labor, the Department of Education, National Science Foundation, and National Institutes of Health. The higher education and agency associations are consistent per the guidance given in the *United States Government Accountability Office (GAO).*

> *To assist in providing these important services, the federal government relies extensively on contractors to provide IT services and systems. In addition to contractors that provide systems and services to the federal government, other organizations possess or use federal information or have access to federal information systems. These other organizations with privileged access to federal data and systems can include grantees, state and local governments, and research and educational institutions. [***44***]*

If compliance is not adhered too, grant recipients may have funding withheld. Similarly, this same principle applies to institutions receiving funding for financial aid and/or research grants from a federally funded agency. Oddly, these very principles often impel attitudes, and it is these attitudes that we will investigate in the following section.

## 5. ATTITUDES AND ACADEMIC FREEDOMS

Having discussed some of the key objectives and associated components and challenges faced by higher education, FISMA's focus is to manage enterprise risk for the federal government and associated agencies. It generalizes the process by suggesting and outlining a six-step strategy for achieving secure information systems. These steps are as follows:

- Categorize (your information and information system)
- Select (the appropriate baseline or minimum-security controls)
- Implement (the security controls in the information system)
- Assess (the effectiveness of the security controls)
- Authorize (information system processing after risk determination)
- Monitor (the security controls on a continuous basis)

These "high level" identifiable steps are typically present in most corporate entities "closed system" technological processes. Higher education on the other hand, may not have graduated their technological processes to the same level of detail due to the open and often wanton attitude that dominates this culture. [***22***] According to Readings, the university system as a whole has in part isolated themselves from mainstream ideologies (to include government) as it strives to become a self-preserving and self-serving entity under the banner of academic freedom.

> *It is no longer clear what role the University plays in society. The structure of the contemporary University is changing rapidly, and we have yet to understand what precisely these changes will mean. Is a new age dawning for the University, the renaissance of higher education under way? Alternatively, is the University in the twilight of its social function, the demise of higher education fast approaching?*

The attitude of isolation in Readings' work expresses itself again with the emotional/mental imagery in Lawrence White's article where he explores the compliance frontier in the future. *Which Legal Issues Will Keep Colleges Busy in the Year 2012* is White's vision where he imagines the challenges 6.6 years ahead saying, "Tomorrow, with federal government extending its tentacles deeper and deeper into higher-education enterprise, compliance may well become the campus lawyer's principle responsibility." This imagery of government as monster helps cement the discourse of academic freedoms as a banner to rally around instead of an ideology to defend.

> *"It's fair to say the institutional autonomy is under relentless assault by legislators, government administrators, and others who presume to know better than faculty members and academic administrators how to make financial, managerial, and even pedagogical judgments affecting campuses." [**23**]*

This us-versus-them point-of-view exposes itself in White's statement. It is these emotional declarations that some in higher education - like White - have expressed dramatic passion in their argument and dogmatic opposition to anything regulatory. This seems to ignore the understanding of the mission of information security as a discipline built upon three tenants: confidentiality, integrity, and availability, and not an effort to curb academic freedom. Moreover, when did higher education define availability as an obstruction to sharing of information and learning? Furthermore, in what research environment does the lack of integrity support research findings? Finally, in what enclave is the loss of copyright and intellectual property acceptable?

White is not alone; he quotes Georgetown University Law Center's professor J. Peter Byrne's definition of academic autonomy as, "a First Amendment right of the university itself –

understood in its corporate capacity – largely to be free from government interference in the performance of core educational functions." [***23***] With attitudes established as an issue, an examination follows of this issue's effects on alignment between higher education and the government followed by the mandates and costs of compliance.

### *Attitudes with Government Alignment*

The challenge higher education faces is the level of influence and involvement of government it should embrace. Authors Ke and Wang make some observations regarding the responsibility and tension that exist.

> *Government is defined as the agent endowed with a monopoly on the use of force…. With the potentially powerful forces, governments can exert influence and regulation over other social entities…. Influence is the exerting of persuasive control over the practices, rules and belief systems under the government's way. Governments can exert influence via education and socialization processes of individuals, the systematic articulation of particular points of view, and provision of differentially more resources to those social activities deemed "appropriate" and withholding of resources from those deemed "inappropriate." In addition, governments can directly or indirectly intervene in the behavior of organizations by using regulations. By regulations, governments can make conflicting, decentralized decisions compatible, control the prevailing mode of resource accumulation and reproduce existing social relationships through a system of historically determined institutional forms. [***45***]*

Institutions in higher education range in form and functionality from research institutions to four year, two year, universities, and colleges. Regardless of the type or focus of a higher educational system, clear criteria to assess security compliance for the safeguarding of

information and information systems must be determined. Wang in his article, *Information Security Models and Metrics*, addresses the precedence for identifiable metrics and a standard measurement criterion.

> *It is widely recognized that metrics are important to information security because we cannot measure the success of security policy, mechanism, or implementations without security metrics. Metrics can be an effective tool for information security professionals to measure the security strength and levels of their systems, products, processes, and readiness to address security issues they are facing. Metrics can also help identify system vulnerabilities, providing guidance in prioritizing corrective actions, and raising the level of security awareness within the organization. With the knowledge of security metrics, an information security professional can answer typical questions like "Are we secure?" and "How secure are we?" in a formal and persuadable manner. For federal agencies, a number of existing laws, rules, and regulations cite security metrics as a requirement…. These laws include the Clinger-Cohen Act,[22] Government Performance and Results Act (GPRA),[23] Government Paperwork Elimination Act (GPEA), and Federal Information Security Management Act (FISMA). Moreover, metrics can be used to justify and direct future security investment. Security metrics can also improve accountability to stakeholders and improve customer confidence. [***46****]*

What is not clear is the response and role that higher education has taken or will take to meet an effective balance of compliance and academic freedoms. Someone, somewhere, will have to make a decision for the information and information systems they support. As discussed earlier in Petersen's *Safeguarding the Assets in Higher Education – the Role of the CSO*,

[22] https://www.fismacenter.com/Clinger%20Cohen.pdf
[23] http://www.whitehouse.gov/omb/mgmt-gpra/gplaw2m

> *The CSO is already a valuable resource in other sectors. The Federal Information Security Management Act (FISMA) mandates that U.S. federal government agencies appoint a CSO. Many state governments have also moved to create an information security function… The private sector too has embraced the CSO function…. [**33**]*

Within this context, the "more open" self-perceived notion is predicated on higher education's embrace of "academic freedoms." Academic freedom is a multi-faceted subject where philosophical, political, economic and civil liberties all influence the subject's timbre. Defined as, "the freedom of teachers, students, and academic institutions to pursue knowledge wherever it may lead, without undue or unreasonable interference," academic freedom's purpose is to "guarantee academics a bastion of free speech and thought, independent of the politics and public sentiment of the day." [***47***]

***Federal Mandates***

"According to the National Conference of State Legislators, data breach notification laws are on the books in 46 states," reports Dian Schaffhauser for *Campus Technology*. "These laws are layered on top of other federal regulations, such as the *Family Educational Rights and Privacy Act* (FERPA) and the *Health Insurance Portability and Accountability Act* (HIPAA). Schaffhauser's opinion is only the beginning. Heidi Wachs, the director of IT policy and the privacy officer for Georgetown University in an interview with Schaffhauser said, "I actually think that the regulatory and compliance hurdles will only increase moving forward." [***48***] Public trust expected of and placed upon higher education regarding data privacy and protection is significant. Yet this trust is disproportionately inflated as it relates to the security of information and information systems. Joseph E. Campana, Ph.D., CIPP/G, CITRMS in his 2008 report *How Safe Are We in Our Schools* reports,

> *The Education Sector, which comprises as little as 0.6% of the total number of U.S. entities, reported a disproportionate number of information security breaches…. The data breach incidents reported by the Education Sector account for more than 12.4 million student and other consumer profiles that were either lost or stolen, or inappropriately accessed, exposed or disposed…. Postsecondary schools – colleges and universities, account for 79% of the breach incidents reported by the Education Sector..., at least 24% were attributed to hacking into information systems. Many others attributed the breach to "unauthorized access," which may include an intrusion by a hacker as well as unauthorized access by an insider or student. Over a third (35%) of the breach incidents were attributed to lost, stolen or missing computers, electronic storage devices, magnetic tapes, microfiche and paper files. Incidences involving computer-related systems and devices accounted for 32% while breaches involving stolen or missing laptop computers accounted for 15% of the total. [***49***]*

However, the metric most important is the number of affected constituents. Examples of the reported incidents occurring in 2010 with affected personnel numbers include:

- Armstrong Atlantic State University - hard drive stolen with nursing student information, hundreds affected;
- Tulane University – laptop stolen with W-2 information, 10,000 affected;
- Saint Louis University – network breached exposing social security numbers, 12,800 affected;
- Stony Brook University – student misconduct posted a list of student names and unique ID numbers after discovering an exploit, 61,101 affected; and

- Ohio State University – server breached exposing social security numbers, 760,000 affected. [***50***]

Table 4 illustrates a snapshot of the affects of an incident by type on data confidentiality, integrity and availability of information and information systems entrusted by higher education.

***Table 4. Incidents and Breaches in Higher Education***

| | **Incidents** | **Breaches** | **By Type:** | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | *Theft* | *Impersonation* | *Loss* | *Penetration* | *Unauthorized Disclosure* | *Employee Fraud* |
| **2006** | 83 | 65 | 26 | 1 | 3 | 33 | 20 | 0 |
| **2007** | 139 | 112 | 39 | 3 | 13 | 30 | 53 | 1 |
| **2008** | 173 | 178 | 40 | 4 | 9 | 35 | 75 | 10 |
| **2009** | 86 | 102 | 22 | 2 | 0 | 29 | 30 | 2 |

"Several sections of the revised *Higher Education Opportunity Act*, signed into law in 2008, deal with unauthorized file sharing on campus networks. Schools have two responsibilities under the law," says Schaffhauser. The first was "to develop, implement, and regularly review written plans to combat unauthorized distribution of copyrighted material by users of the institution's network." The second was "to inform and educate their communities about the appropriate use of copyrighted materials." [***48***]

The federal government has quickly learned of the results of public distrust and has taken measures to securely position trust and displace public opinion liability with the enactment of FISMA. Just as an enterprise needs to protect itself, its suppliers, and its customers, the government must protect its systems and its citizens from security threats, both physically and in

cyberspace. Local and national governments cannot afford to have major crises such as interruption of operations that are based on computers, loss of confidential data, or theft of computing resources. Security incidents that are well-publicized lead to a diminution of public trust and present an obstacle to promotion of e-government initiatives. Therefore, government's first responsibility in terms of computer security is probably to "get its own house in order," meaning that government agencies at all levels (state, regional, local and tribal entities) must protect the information and information systems that they own and operate.

What is not certain is how higher education from its "ivory tower" will respond when public opinion wanes due to the many security breaches or exploitations of information and information systems from negligence or non-compliance. Higher education traditionally would lead the way for government to follow. Paradoxical as it may seem, higher education has failed to censor its technological freedoms, which might ultimately be at its own expense. The Corporate Information Security Working Group supports this view by stating:

> *It is imperative that public and private sector organizations protect the information entrusted to them by various stakeholders against unauthorized access, disclosure, use, loss, or damage. Not only is this a basic fiduciary responsibility, but a growing body of external requirements mandates attention to information security. [***51***]*

As others have noted, they likewise suggested that the application of FISMA compliance would not hinder productivity, but benefit the organization's security program.

> *Organizations are encouraged to use voluntarily this guidance as a resource whether seeking to initiate a new information security program or enhance an existing program. The use of these information security practices and supporting metrics will enable enterprises everywhere to better protect themselves from financial, operational, or*

> *reputational damage or loss resulting from unauthorized access, disclosure or use of the information entrusted to them by their stakeholders. [***51***]*

Are the federal regulatory mandates having an impact? Many in higher education are slowly recognizing that information and information system security is paramount, versus optional, and must be given more attention. Voloudakis, a speaker from EDUCAUSE, in *The Continuing Evolution of Effective IT Security Practices,* references Robert Kvavik from his article *Safeguarding the Tower: IT Security in Higher Education* and states the following,

> *Pressure to improve security is coming not only from inside the institution, in response to more malevolent threats. Compliance with a growing list of existing and emerging federal and state laws and regulations is certain to be another, external driver of change.* [***11***]

Examples of these laws and regulations that do come into play and given consideration of the scope of higher education's information and information system security include:

- The Family Educational Rights and Privacy Act (FERPA); [24]
- The FTC safeguards regulations of the Gramm-Leach-Bliley Act (GLBA); [25]
- The Health Insurance Portability and Accountability Act (HIPAA); [26]
- State laws on notification of security breach;
- The Electronic Communications Privacy Act (ECPA); [27]
- The TEACH Act, allows liberal application of copying materials for instruction, but also implies an obligation for privacy and security; [28]
- The Digital Millennium Copyright Act (DMCA), can circumvent protection measures; [29]

[24] http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
[25] http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act
[26] http://www.hhs.gov/ocr/privacy
[27] http://www.law.cornell.edu/uscode/18/usc_sup_01_18_10_I_20_119.htm
[28] http://thomas.loc.gov/cgi-bin/cpquery/z?cp107:sr103

- The USA PATRIOT ACT (section 215), cannot reveal investigations by government agencies and allows seizing of business records; [30]
- The FDA rule on electronic records and electronic signatures (21 C.F.R. Part 11); [31] and
- The Payment Card Industry Data Security Standard (PCI-DSS). [32]

Voloudakis goes on further to comment that FISMA was legislated to mandate compliance to ensure that a consistent set of standards and practices would be put in place for the safeguarding of information and information systems of federally controlled systems. [***11***]

Higher education is not currently required to comply with FISMA's federal requirements – that is the legislation is federally focused. As mentioned before, there are enclaves or end-nodes within higher education that may be compliant as they are extensions to a protected environment. However, these are exceptions. It is just a matter of time before particulars of the law take precedence as cases move through the courts. Once this identification process is complete through legal challenge, it may no longer be an option for compliance, but an obligation. Higher education can be proactive and join – even take a leadership position in – the movement towards a more unified application of information and information systems security standardization. The process for doing so is referred to as the Information Security and Privacy Advisory Board (ISPAB). The ISPAB was originally created by the *Computer Security Act of 1987* (P.L. 100-235) as the Computer System Security and Privacy Advisory Board. Because of Public Law 107-347, *The E-Government Act of 2002*, Title III, *The Federal Information Security Management Act of 2002*, the advisory board changed its name and amended its mandate. The advisory board's objectives include:

---

[29] http://www.copyright.gov/legislation/dmca.pdf
[30] http://epic.org/privacy/terrorism/hr3162.html
[31] http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11
[32] https://www.pcisecuritystandards.org/ - PCI is not a federal statute; it is an industry attempt at self-regulation.

- Identify emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy;
- Advise the National Institute of Standards and Technology (NIST), the Secretary of Commerce and the Director of the Office of Management and Budget on information security and privacy issues pertaining to Federal Government information systems, including thorough review of proposed standards and guidelines developed by NIST.
- Annually report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency and the appropriate committees of the Congress.

As for the scope, the advisory board's authority does not extend to private sector systems or federal systems, which process classified information. Their objectives and duties include:

- The membership of the Board consists of twelve members and a Chairperson.
- The Director of NIST approves membership appointments and appoints the Chairperson.
- The Board meets quarterly throughout the year and all meetings are open to the public.
- The Board invites public comments on its activities and the objectives the Board should undertake. [***52***]

The site consists of a *Membership* link, which has the contact information. Examples of those that have agreed to participate in ISPAB come from such companies as:

- IBM Center for The Business of Government;
- Computer Science Department University of Massachusetts Amherst;
- U.S. Army War College;
- U.S. Department of Treasury;
- McAfee;

- Social Security Administration;
- Google; and,
- Microsoft – to name a few.

Links also available are *Meetings, News & Events, Activities,* and a *Documentation* library, which dates back to April 9, 2001. As seen above, many private industries and agencies are realizing the value. According to Gartner,

> *Government organizations that are required to meet FISMA compliance should use [compliance] as a control framework … and for asset clarification. Use compliance as an opportunity to improve operational security not only by defining assets and documenting the current state of the organization, but also by implementing control objectives that drive effective risk analysis and management. Moreover, organizations should use compliance as an opportunity to implement technologies and processes that improve operational security as well as provide support for FISMA and FIPS 199 compliance. [***53***]*

Other companies marketing products are gearing up to meet compliance requirements as they clearly acknowledge the federal mandate.

> *Laws to protect the confidentiality, integrity and availability of information and systems that support the operations and assets of government agencies mandate compliance with FISMA. Agencies failing to meet FISMA requirements face withholding of federal funds and withdrawal of contractor eligibility status. FISMA requires federal agencies to develop, document, and implement agency-wide information security programs. All U.S. government federal agencies and qualifying organizations contracted on behalf of U.S. government agencies must conform to FISMA's mandatory processes. [***54***]*

Examples include VeriSign, [33] which offers consulting services and the ability to leverage its own Security Operations Center staffed by CISSP's [34] around the clock; whereas, netForensics provides a tool called nFX to provide federal agencies an efficient and effective means to report FISMA compliance. [***42***] [***55***] However, all of these mandates and the tools to measure success (thinking positively) are unfunded. Where is higher education going to find the funding for compliance?

***The Cost of Compliance***

Has higher education considered the implications FISMA has identified? Rodney Petersen and Jack Suess, in March 2008, *Briefing to CSIS Commission on Cyber Security* sum up the situation quite clearly.

> *Data security breaches combined with several states enacting security breach notification laws have forced institutions of higher education to take a serious look at how they handle notifications following incidents. More importantly, they are working to prevent data exposures in the first place through aggressive data protection initiatives. [**4**]*

The cost involved in FISMA compliance is nominal compared to the expense of ignoring the risk of compromise associated with information and information systems. Peterson and Suess continue to articulate the benefits of the FISMA framework – first introduced a year earlier – by stating,

> *It is difficult for nonprofit organizations to build the costs for security into the products and services they sell. At a time when state funding is declining and rising tuition prices are under increased scrutiny, colleges and universities as nonprofit organizations must*

[33] http://www.verisign.com/
[34] Certified Information Systems Security Professional – https://www.isc2.org/

> *be creative and resourceful in addressing the cyber security challenge… In that regard, NIST has been an invaluable resource to the nonprofit sector. NIST standards and guidelines, especially the 800 series, are highly valued resources within the higher education community…. [**4**]*

The aforementioned companies that provide "FISMA Compliant" services covering such tasks as security incident and event management (SIEM) or alerting and archiving services represent quantifiable values not often thought of in the early phases of development. Since HSPD-12, digital reporting through access control measures (PIV)[35] of real-time logs via the service in question to the reporting agent using a continuous monitoring model and SCAP [36] has proven to be the method supported and directed by the federal government. [***17***] [***56***] [***57***]

There is much to consider when assessing where higher education is in the information and information systems security program process. Regarding the protection of higher education's critical infrastructure protection, Rodney and Suess state that the federal government efforts to improve critical infrastructure protection and implement the *Federal Information Systems Management Act (FISMA)* may affect higher education's resources and ability to conduct federally funded research. [***4***] Yet it is EDUCAUSE's policy position that "their unique social position between the commercial and government sectors, institutions of higher learning have the opportunity to show how critical infrastructure protection and security can be accomplished in a diverse, complex, and dynamic environment while still maintaining essential freedoms… and preclude the need for "top-down," cumbersome, federal regulation. They continue by stating EDUCAUSE's objective is to bring a level of awareness by "working to educate the broader community on need for more robust IT security." [***58***] Yet, in the preceding statement the "ivory

[35] Personal Identity Verification
[36] Security Content Automation Program

tower" culture and mind-set, is being guarded in their approach, and remains steadfast with their declaration of self-sustained autonomy, which is at odds with the request to be considered a "critical asset." Being a critical asset makes higher education responsible and eligible for federal dollars and oversight. Ultimately, regulation and compliance should support and make the various business functions more fluid, effective, and secure. What the mandates should not do is impose inflexible, inflated systems with unnecessary requirements; that produce rotund, slow, and ineffective information systems unable to support their intended purpose. Unfortunately, this is exactly FISMA's characterization prior to 2010's shift from a paper-based reporting model to the digital model in support of the *Government Paperwork Elimination Act, Paperwork Reduction Act*, and the OMB. [***59***] [***60***] However, funding remains an issue unresolved and "unfunded mandates" continues to be a concern heard in the halls of higher education.

The following section presents an overview of existing federal and state privacy and security related laws affecting institutions of higher education. The objective is to discuss the practical implications of such laws for institutions of higher education and suggests areas for further exploration and development of effective processes to meet the FISMA challenge.

## 6. LEGAL CHALLENGES

*"*New more prescriptive laws and regulations affording greater protection to personal information are based on the very real threats posed by identity thieves, scam artists and crooks who are stealing credit and debit-card numbers, health plan data, and bank account information and the like that reside in disparate databases and are transmitted over the Internet. Unfortunately, personal information often is compromised because basic information security controls – such as strong passwords, encryption and up-to-date anti-virus software - are not in place, or because the resources and sophistication of cyber-criminals often seriously exceed those of the public and private sectors." [***61***]

The tension to provide academic information technology systems for faculty, staff and student use with open accessibility, versus the need for operational, business-oriented enterprise systems where "legal compliance, data confidentiality, and security are paramount" has become a fiduciary responsibility. [***2***]

> *Basic fiduciary responsibilities include protection of shareholder interest, compliance with external requirements, and oversight of internal and external audits, all of which have information security implications. A balanced Information Security Program embraces a carefully selected set of foundational principles…, upon which management can build a structure of security policies, processes, controls, and performance metrics…, the first step is to identify and list all information assets, properly classified with respect to confidentiality, integrity, availability, and privacy considerations. [***51***]*

Moreover, "hacker attacks… can produce more than inconveniences for institutions: they can also produce liability lawsuits…. Hacker attacks are just one of several ways that information technology and the Internet have broadened colleges' liability potential." [***62***]

***Reputation and Trust***

*Diligence is the nebulous factor that is key in demonstrating that others should put their trust in you…. [**63**]*

Recall in *Federal Mandates,* public trust expected of and placed upon higher education is significant. Yet this trust is disproportionately inflated as it relates to the security of information and information systems. The federal government has quickly learned of the results of public distrust and has taken measures to securely position trust and displace public opinion liability with the enactment of FISMA. Has higher education? On this subject, Andrea Foster's article *Insecure and Unaware* says,

> *Security lapses are common at colleges. It is a conclusion shared by experts on campus-computer security, some of whom worry that colleges could eventually be sued for operating their information systems negligently. [**64**]*

When addressing leadership attitudes, Foster states, "What I have seen is a top-to-bottom lack of awareness of issues related to security." In addition, when expounding on attitudes towards responsibilities, Foster exclaims, "You have faculty who believe that because it is their machine and because of academic freedom, they should be able to do whatever they want." [***64***] EDUCAUSE adds, "ISO's reported that the faculty members they interact with demonstrate a desire for independence from central authority, a tendency to reject centrally mandated policy, and an attachment to intellectual freedom as a reason to assume utilization of technology in an unfettered way." [***1***] Eugene Schultz, editor in chief of the journal *Computers & Security* agrees with Foster's assessment and says universities are, "among the least secure places in the universe, as far as computing goes." [***64***] Florence Olsen's *The Growing Vulnerability of Campus Networks* 2002 article for *The Chronicle of Higher Education* quotes the vice president

for information technology at Indiana University's Michael A. McRobbie, which supports Foster's view. McRobbie says,

> *Colleges have a well-deserved reputation for lax network security. As a result, they risk increased insurance costs and expensive lawsuits…. In a time of increased national-security concerns…, pressure is mounting on colleges to gain better control of their computer networks, or risk losing federal grant money for research. [***65***]*

Again, recall in A*ttitudes with Government Alignment,* someone, somewhere, will have to make a decision for the information and information systems they support. McRobbie, in a speech said, "In the present climate of cyber-threats, somebody in the university has to step forward and take responsibility for trying to remediate these threats and to translate what the risks are." Olsen sums up the affects for failure to perform such remediation saying,

> *Colleges could be subject to a costly negligence lawsuit if their computers are used in future attacks, or sensitive information about students is stolen from campus computers… Courts may find colleges liable for an attack that used their machines, because campus officials should have known that unsecured networks were open to attack. [***65***]*

Is reputation and trust "really" that important? Foster quotes Mr. Vinik, of United Educators to say, "Because of the prevalence of security mishaps, it may be just a matter of time before colleges are hit with multimillion-dollar lawsuits accusing them of negligently operating their networks…. Prevention and risk management is key…, because if you were to be sued and somebody says that you did not have adequate security, you want to be able to show that you engaged in significant audit-type measures and tried to correct problems." [***64***]

Are administrators of higher education cognizant of the challenges and responsibilities of law and compliance in regards to information and information systems security, and if so do they

act in the best interest of the institution with awareness of compliance as a guide? The following section suggests maybe not. Litigation against higher education institutions with the charge of negligence continues to escalate. Understanding the effects of negligence and the duties of care that accompany it are collectively critical in accepting the new legal environment and limiting risk exposure to lawsuits.

### *Challenges of Law and Compliance*

"Many university administrators feel as if they are lost in a shadowy forest of quickly growing federal regulations." [***66***] Again, here is the use of foreboding imagery; however, the potential absence of standards, which could leave an institution floundering in indecision, is really the benefit provided to higher education or other agencies who embrace the FISMA processes. Salomon, Cassat, & Thibeau warn that if appropriate measures to safeguard information and information systems per the guidance given through federal and state regulatory compliance requirements are not adhered to that,

> *[In] many cases, institutions remain subject to suits based on common law negligence theories. In fact, as distance education and information technology have enabled colleges and universities to spread their reaches even farther, institutions may be subject to suit in multiple states and even foreign jurisdictions. The likelihood that multiple federal, state and foreign laws could apply is even greater when it comes to laws that relate to the use or misuse of information technology. [**3**]*

As mentioned above, federal jurisdiction is but one facet considered when contemplating the scope of compliance.

> *Institutions naturally tend to worry most about federal requirements that constrain their actions or increase their cost. In addition to the variety of federal laws that are*

> *applicable to information security and privacy, there are numerous state laws relating to security and privacy…. Compliance with state laws is even more challenging in the context of technology-mediated learning: an e-learning student residing in one state may be protected by a set of laws that are different from the ones that apply to the state where the institution he or she is attending is located, and vice versa. As a result, the student may become subject to laws very different from those of his or her home state. Where once an institution could be more content with the understanding of federal legal requirements and those of its state of domicile they are now finding it necessary to extend their knowledge base nationally and, indeed, globally.* [***3***]

Regardless of the environment of compliance and potential for litigious pursuit in the event of breach and the increasing evidence of the need for regulation and application of repeatable and actionable controls for the safeguard of information and information systems, Kelly Field's September 2011 article in *The Chronicle of Higher Learning* expresses clearly the attitude of higher education in relation to federal regulatory requirements stating, "Colleges feel burdened by federal regulation…[Moreover] that the government's "regulatory-burden calculations" underestimates the burden that complying with the federal rules places on colleges." [***67***] As a result, institutions over-burdened may tolerate a defeated or ineffectual attitude. Salomon (et. al.) addresses the challenge of how higher education often empowers delinquent activities due to negligence or failed oversight.

> *Not only can an educational institution's computer systems be the target of unauthorized access from outside the institution, but also individuals with access to those powerful systems can use them to launch unauthorized attacks on other computer systems and networks. Public access terminals located in college and university libraries, now a*

> *nearly universal phenomenon, are particularly vulnerable, both as a means to obtain access to institutional networks and to harass others anonymously. [**3**]*

In addition, Salomon (et. al.) identify the liability associated with this abuse within the context of the legal system for those institutions who fail to take the proper measures to safeguard their information and information systems,

> *As a result of these trends, college and university administrators, IT professionals, and legal counsel should become familiar with the federal and state computer theft and privacy laws that may give rise to criminal prosecution or civil claims against the institution as well as its personnel and students…, [also consider that] state computer crime laws and common law or statutory rights of privacy may be implicated in situations where improper access is gained to a supposedly secure computer system. [**3**]*

Another challenge to compliance is risk management / incident response. "The worst time to prepare for a response to a security failure involving unauthorized disclosure of educational records or other personal information is after it happens." Moreover, developing a risk management program exclusive of a fully matured program with repeatable and actionable controls contains no guarantees. "In fact, by identifying an institution's vulnerability to unauthorized access to its electronic records, without then promptly instituting appropriate measures to remedy those vulnerabilities, the institution may only serve to heighten its potential liability should the compromise occur."

"An increasingly adversarial mind-set, a decrease in civility and a diminishing level of trust in all social institutions have made it more acceptable for people to assert legal claims at the slightest provocation." [***68***] This is a litigious society. "Many of the costs and potential liabilities associated with the increasingly complex challenges faced by educational institutions

are in the areas of information privacy and security result from the absence of uniform standards…. Absent such standards, institutions remain vulnerable to class action challenges in the event their information security policies and procedures fail to repel unauthorized intruders." [***3***]

"Lawsuits can divert colleges from their primary missions of teaching, research, and service." [***68***] The paradox exists, "dammed-if-you do, dammed-if-you-don't." Divert time to securing the environment, or divert time to litigious pursuits. "Educational institutions at all levels would be far better served through the development and adoption of guidance in the form of recommended "best practices" or similar measures." [***3***] Institutions of higher education can reduce this potential by better understanding the legal environment, and to that end, know the risks to the threats indentified during the last risk assessment.

***Legal Liability – Duty of Care***

Risk is defined primarily in fiscal terms – that is quantitatively. Institutions of higher education that access federally protected information and information systems must address FISMA compliance in terms of "How much does it cost if we fail to comply or mitigate risk?" Author Anne Payton in her article *Data Security Breach: Seeking a Prescription for Adequate Remedy* clearly highlights the technical responsibilities as it relates to legal liability.

> *Part of the responsibility for information…is with the party responsible for the information's care. Were it not for the inadequate security measures making private information available to thieves, the identity theft would not have occurred…. When a party fails its custodial duties in such a blatant manner, it would seem that owners of the assets put at risk have a clear right to charge of negligence. In tort cases, negligence is determined by asking these basic questions:*

> *1. Does the defendant owe a duty of care to the plaintiff?*
>
> *2. Did the defendant breach that duty?*
>
> *3. Did the plaintiff suffer a legally recognizable injury due to the defendant's breach?*
>
> *4. Did the defendant's breach cause the plaintiff's injury?*
>
> *They owe a duty of care to these parties to maintain secure transactions or services, to the intermediary, and by extension to the data owner involved in the service. [**69**]*

Compliance with FISMA standards will not guarantee elimination of risk, but it will certainly limit the level of liability and put in place universally recognized standards and security practices to help mitigate loss.

Authors Romney & Romney in an article titled *Neglect of Information Privacy Instruction – a Case of Educational Malpractice* highlight the shortsightedness of the educational system to empower effectively students to meet the challenge of information security and influence our society's information technology social systems.

> *Not only should information technology educators be knowledgeable regarding data privacy legislation but also they should be teaching correct system and database design principles to IT students in order to ensure future application design compliance with international legislative trends…. In the legal field, malpractice is commonly considered to consist of a failure of competence or thoroughness that result in economic, legal or commercial damage to someone reasonably relying on the professional services. [**70**]*

The implication of this statement is the very contexts in which higher education trains their students contradicts the real-world they will enter to support and secure in the work force. Higher education must take a stand on what standards they are to use and how they are applied.

After citing many federal regulatory requirements, such as the Electronic Communications Privacy Act (ECPA), the Computer Fraud and Abuse Act (CFAA), and the Family Educational Rights and Privacy Act (FERPA) authors Salomon, Cassat, & Thibeau continue with the following comments.

> *In many ways, however, these laws have failed to keep pace with technological innovations. The result has been an atmosphere of uncertainty, placing further strain on already scarce institutional resources and leading in some cases to inaction because of concerns over legal exposure. The absence of a single set of standards further complicates the issue, leaving administrators and IT directors struggling to decide how best to protect their institutions while at the same time not interfering with their educational mission. [**3**]*

Margaret O'Donnell and Craig Parker's observation in *How Colleges Can Navigate the Thicket of Federal Regulations* states well the challenges ahead for higher education and the need to meet compliance where required. "Penalties, fines, litigation, and institutional embarrassment, while important, are not the best reasons for colleges to comply. The regulations are mechanisms to uphold important values on our campuses – maintaining privacy and confidentiality, protecting intellectual property and academic freedom, promoting the safety and dignity of every person, providing each an equal opportunity to participate in campus life. A campus "culture of compliance" is needed to preserve the core values underlying federal regulations." [***66***]

### *Real-World Examples of Neglect*

Recall, what is not certain is how higher education from its "ivory tower" will respond when public opinion wanes due to the many security breaches or exploitations of information

and information systems from negligence or non-compliance. Higher education traditionally would lead the way for government to follow. Paradoxical as it may seem, higher education has failed to censor its technological freedoms, which might ultimately be at its own expense. Addressing this issue, The Corporate Information Security Working Group states:

> *It is imperative that public and private sector organizations protect the information entrusted to them by various stakeholders against unauthorized access, disclosure, use, loss, or damage. Not only is this a basic fiduciary responsibility, but a growing body of external requirements mandates attention to information security. [**51**]*

A real-world example of higher education and the potential for negligence charges is Ohio University. "Two of those affected have sued the university for negligence in not keeping their Social Security numbers and other personal data safe…. The suit would be the first of its kind against a college and could spur more colleges to buy cyber insurance." [***71***] In a January 2010 article for *The Chronicle of Higher Education*, Mary Helen Miller reports on a study conducted by the Ponemon Institute that expresses the cost of addressing data breaches is increasing. [***72***]

> *The suit, filed last summer, charged Ohio [University] with negligence and asked the university to pay for credit-monitoring services for anyone whose personal information was left unprotected. [Nevertheless,] a judge with the Ohio Court of Claims dismissed the suit yesterday, ruling that the alumni had not proved that they suffered any real damages from the computer-security breaches…; there is no evidence that anyone whose personal data were exposed has been the victim of fraud or identity theft, according to campus officials. [**73**]*

As stated in the aforementioned section, in tort cases, negligence is determined dependent on the answers to these questions:

1. Does the defendant owe a duty of care to the plaintiff?
2. Did the defendant breach that duty?
3. Did the plaintiff suffer a legally recognizable injury due to the defendant's breach?
4. Did the defendant's breach cause the plaintiff's injury?

As decided above, the judge did not get an adequate answer to find the plaintiff (the alumni) had suffered an injury. Was there injury? If one were to ask the students of Ohio University, the answer would appear to be yes – a loss of trust. Referencing the Ohio University's network breach, "The student newspaper, *The Post*, reacted angrily to the latest breach in an editorial. 'Whether through oversight, negligence, a false sense of security or any other means, Ohio University has failed to protect those closest to it.'" [***74***]

This is far from the only example. For instance, "The University of North Carolina at Chapel Hill and Bonnie Yankaskas, an epidemiologist, have settled a dispute over the extent to which she was responsible for a security breach in a computer database used for her studies on breast cancer." Doug Lederman, in his 2011 article titled *Chapel Hill, Researcher Settle Dispute on Computer Security* reported that the "university…held Yankaskas responsible, and demoted her from full to associate professor…. Under the settlement, she is returning to full professor and her full professor's salary, but will retire at the end of the year." Lederman goes on to print the joint statement - in part - on the settlement is as follows:

> *Dr. Yankaskas acknowledges that…she had the responsibility for the scientific, fiscal and ethical conduct of the project, and responsibility to hire and supervise the [Carolina Mammography Registry] CMR information technology staff who, with assistance as*

> *requested from School of Medicine and University information technology professionals, operate and maintain the CMR computer systems on which secure data are maintained." [**75**]*

"The dispute" reports Eric Ferreri, "centered on what university officials said was the scientist's failure to secure a server housing much of that data, including about 114,000 Social Security numbers… Although the university doesn't think any personal information was removed, it nonetheless notified all 180,000 women with data on the server and set up a call center to answer questions once word of the breach got out. Doing so cost roughly $250,000, officials say." [***76***] The aforementioned is an example of negligence (duty, breach, injury, and damages) that did not appear before the court. Moreover, it appears the incident was tried within the halls of academe.

In contrast to the earlier examples, Josh Keller's November 2010 *Former Student Sues U. of Hawaii over Data Breaches* article explored an incident where a student named Philippe Gross filed suit against a university for breach of privacy. Keller reported,

> *Are colleges that expose confidential student records vulnerable to class-action lawsuits…? [A] former student at the University of Hawaii-Manoa filed a class-action suit on Thursday against the University of Hawaii after the system allowed a series of privacy breaches…. The case could face a difficult road ahead…. An increased risk of identity theft does not constitute an injury, several courts have ruled.*

Again, as stated above, negligence is determined dependent on the answers of the questions surrounding duty and injury - was injury suffered, and was injury caused by the breach of duty? Keller reported that Mr. Grande, the attorney representing Mr. Gross, acknowledged some of the challenges…he pointed to a local case, Arakawa v. Sakata, in which a federal district judge in Hawaii ruled in 2001 that a public agency had violated a motorist's right to privacy when it

released his personal information after a car accident. Mr. Grande continues by stating, "It's a cutting-edge area of the law…I think, in our particular case, we have a very winning argument based on our local precedent to say that our present damages are necessary to prevent future harm." [***77***]

Further research of this incident exposed the extent to which the University of Hawaii was negligent. According to Stefanie Hoffman's report, more than 40,000 former students had their confidential records were exposed, which included such personal information as their social security numbers, grades, dates of birth and other personally identifiable information (PII). The PII exposure was online-based in excess of a year before being discovered by the Liberty Coalition. The breach in security was a result of a faculty member who placed PII on an unsecured server. This was the second of such breaches, the first exposed 53,000 records, while a third exposed 15,000 records because of an infected and compromised system. [***78***] Because of such losses, a class action lawsuit was leveraged against the university in which a "judge has approved the University of Hawaii's settlement over a major data breach involving thousands of students, faculty, and alumni and employees." In a February 16, 2012, news article from KFVE (K5-The Home Team), the reporter states,

> *Under the class action settlement, all of those people will be offered two years of credit monitoring and fraud restoration services.*

The article went on to report that,

> *An attorney who represented the class of plaintiffs calls the settlement "historic." [**79**]*

Historic indeed and precedent setting! Within the article, a posted URL to a site where contact information, phone numbers, and e-mail addresses to seek information for those affected by

these breaches was identified. It appears by this site that five different breaches had taken place. [***80***]

One can extrapolate through these examples that legal interpretation for the negligence of information and information systems concerning security and organizational responsibilities vary from tort law to self-governance and from unknown and untested to tried and precedent setting case law. Understanding the challenges of law and compliance, as stated before, is like hitting moving targets. One must know and implement the fundamentals first to be even able to focus on and eventually hit the item being aimed at – in these cases fundament information security practices. With a renewed understanding of law, duty, and negligence as applied to information security practices, the following section will discuss the key issues higher education has with FISMA and objective alignment and the challenges faced in compliance.

## 7. OBSERVATIONS

### *Objections to and Defense of FISMA*

For *Federal Computer Week*, Brian Robinson in his article *FISMA Compliance Falls Short of Adequate Security* says compliance has, "become a very visible game of political football. Government executives do not want their agencies to receive a D or an F on the House Oversight and Government Reform Committee's annual FISMA compliance score card that's compiled from data that agencies provide to the Office of Management and Budget." It is this fact that Robinson says the crux of the main criticism lies where, "observers both inside and outside government have leveled at regulations such as FISMA: Agencies hustle to get as good a rating as they can each year, but even an A+ doesn't guarantee that IT systems are secure…. It has become a seductive alternate for real IT security, said Rob Lee, a director at information security consultant Mandiant and the curriculum lead for digital forensic training at the SANS Institute. [***81***] To better illustrate this "political football," Congressman Tom Davis of Virginia in 2005 suggested that funding be cut from agencies that fail to improve security; in fact, he said, "FISMA report cards are going to have to be tied to funding… that's the only way to get [the agencies] attention." However, one can see that this is flawed; cutting funds may in fact lead to fewer resources needed to secure the information and information systems as dictated by law. [***82***] SCMagazine.com's Frank Washkuch Jr. expressed his objections when he posed the question in an article titled *Is FISMA Fixable?* Washkuch reported, "Cybersecurity experts with opinions on FISMA are plentiful, many claiming that the law forces government employees to spend too much time preparing for the inspector general, instead of working to improve security." It appears that limited resources are again the center of the complaints… in this example it is time and human effort. "I've had CISO's in significant government agencies saying, 'I'm spending more time and money on FISMA than the actual security itself,'" says

Washbuch. Here again the suggestion of monetary penalties for failure to improve information and information systems security was introduced, but Washbuch states, "I don't think that losing funding is an answer because the lack of funding could be a reason that they're getting bad grades." There are plenty of naysayers who object to the implementation of FISMA for sound reasons – so it appears. However, there are those who feel the implementation of FISMA has matured the information security programs within government – the following is such an example. [***83***]

In defense of FISMA are Nextgov's Tom Davis – yes, the very same congressional representative Tom Davis mentioned above but five years later – and JR Reagan. In their article titled *Analysis: in Defense of FISMA,* they argued that, "despite earlier measures such as the 1987 *Computer Security Act*, the 1996 *Clinger-Cohen Act* and the 2000 *Government Information Security Reform Act*, federal IT security considerations were inadequate prior to FISMA." Congressman Davis and Reagan argued that prior to FISMA,

> *"There was no overarching framework for required security measures and no oversight model to track implementation. In addition, all too frequently, federal systems were designed and procured solely with features and functionality in mind -- not security." FISMA changed this and in many ways brought federal IT professionals into the modern world…. The law:*
>
> - *Explicitly calls out the importance of Cybersecurity;*
> - *Requires an inventory of an agency's IT systems;*
> - *Assigns broad areas of responsibility that continue to work effectively today; and,*
> - *Allows for change over time, as evidenced by the evolving White House and Homeland Security Department roles. [**84**]*

Time has a way of maturing one's views toward information security, and the benefits that a mature program can bring to the protection of information and information systems. The following section is an exploration FISMA's security maturity model and how it applies to and benefits higher education.

***Security Maturity Model***

"A maturity model is a structured collection of elements that describe certain aspects of maturity in an organization," says Martie Lessing of the Council for Scientific and Industrial Research. "This type of security model indicates the degree of development and the strength of the organization's security measures, and provides an organization with a distinct security framework." Lessing further lists how the security maturity models has enabled organizations to:

- generate reproducible and valid measurements;
- establish actual progress in the security milieu;
- rank themselves against a range of organizations;
- determine the order in which security controls should be applied; and
- determine the resources needed to apply to the security programme.

An example of Lessing's security maturity model is the National Institute of Standards and Technology, Computer Security Expert Assist Team Security Maturity Model (NIST CSEAT IT SMM)…, which is inclusive of the Federal Information Processing Standards and Special Publication documentation… that provides implementing organizations with standardized and approved configuration checklists. [***85***] Another example developed was the Software Engineering Institute's (SEI) Capability Maturity Model (CMM), which found its greatest uptake in large organizations such as governments and government contractors to improve the use of

maturity as a measurable means. CMM integrated capability models for software development, systems engineering, integrated product and process development, acquisitions, and security. CMM provides a systematic way of improving processes through effectively classifying organizations by their capability to control critical processes. [***86***] The goal is to achieve a level of discipline that provides for continuous improvement in the overall development process. FISMA through its Program Review for Information Security Management Assistance (PRISMA) utilizes this concept. [***87***] Gartner adopted this model (Figure 2.) and altered it to best support information security practices. The five levels of maturity are:

- *Maturity Level 0: "No Recognizable Process"*
- *Maturity Level 1: Initial (Ad-Hoc)*
    - "Ad hoc" is often used to describe processes at this maturity level. The organization does not provide stability in its processes. Success depends upon individual competence, motivation, and effort, which is not to suggest that the organization is failing to perform the measured tasks, but there is no formal process in place.
- *Maturity Level 2: Developing*
    - Requirements are managed; processes are planned, performed, measured, controlled and documented. Project management is used; discipline is present to ensure that practices endure in times of stress (i.e. *Emergency Operations Plan* / *Disaster Recovery Plan* / *Incident Response Plan*). Project status and delivery is visible, for example, major milestones.

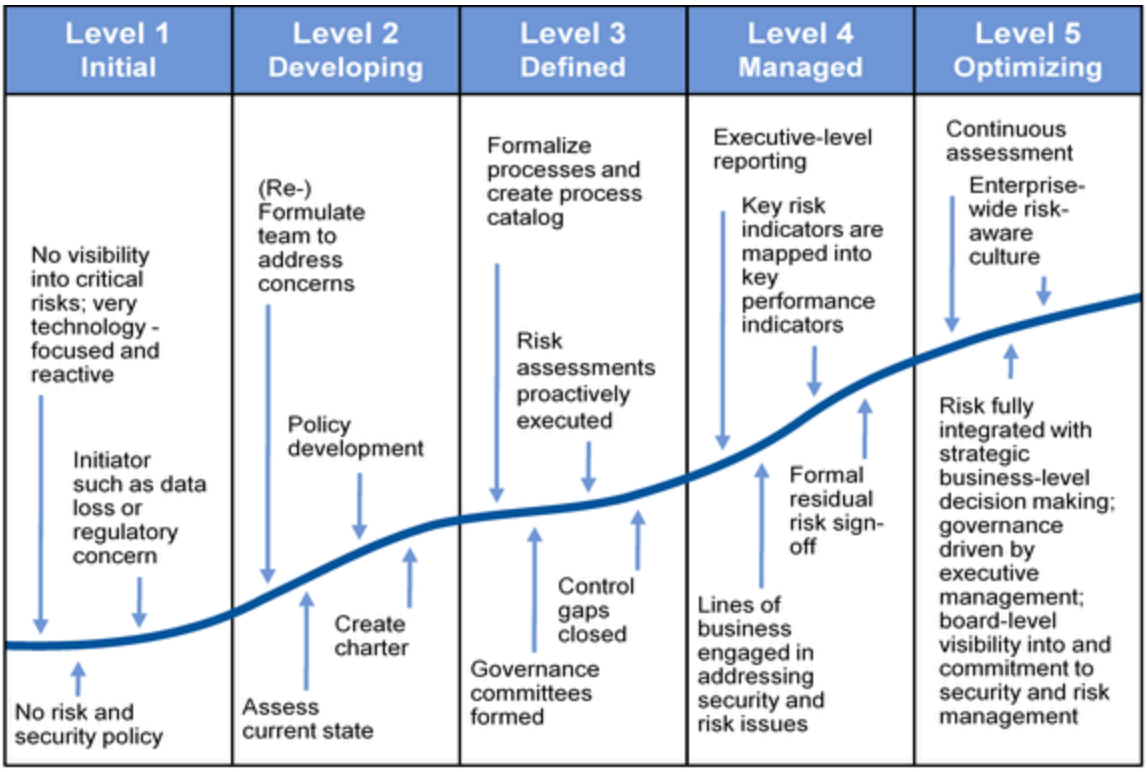


***Figure 2. Security Maturity Model***

- *Maturity Level 3: Defined*
    - Development processes are standardized, well documented, and understood to provide consistency across the organization. Management establishes project objectives based on standard processes, and ensures that these goals are addressed. Standards and procedures for projects are derived from organizational standards to suit that particular project. Each process will be described in more detail and with more rigor. Management is expected to understand relationships between processes and to collect detailed metrics of performance.
- *Maturity Level 4: Managed*
    - Maturity level four organizations use quantitative metrics, including statistics, to control key processes/sub processes and introduced precise measurements into the

process. Numeric goals are established for quality and performance, and are used in process management. Detailed measures of performance are collected, analyzed, and archived for future reference. The critical distinction between level 3 and level 4 organizations is predictable performance.

- *Maturity Level 5: Optimizing*
    - Organizations at maturity level five have developed continually improving process performance, based on a detailed understanding of the relationships between the processes and quantitative monitoring of process performance. Quantitative goals for process improvement for the organization are established, revised as business requirements change, and used in the managing projects. Process improvements are identified, analyzed, and implemented to address the organization's most common issues. This is the level where Information Security becomes Information Assurance. [***88***]

One can see that a standardized model to measure maturity of a program's information and information systems security is beneficial to any organization's information security program. In such a model, the size and scope of the agency or institution of higher education influences the outcome minutely – as the saying goes, "apples-to-apples." Larger organization may take longer to implement the security controls needed to meet the requirements identified through the risk assessment phase mentioned earlier within this paper, but the controls used to mitigate the risks as a result of the existence of a threat and the potential for a subject to exercise a vulnerability in large and small environments remains the same. Moreover, this familiarity makes implementing security measures like FISMA so appealing to many.

***Key Issues with FISMA and Alignment of Objectives***

Who is the *Federal Information Security Management Act (FISMA)* compliance requirements intended audience? As identified earlier, FISMA clearly implies a level of information and information systems security stewardship, which for many academic institutions, practical implementation are not being applied or considered. In general, higher educational institutions would like to maintain security metric flexibility unhindered by federal regulatory compliance. Clearly all federal agencies will have to comply, versus a limited application by educational entities will be required, as applicable for grants and associated funding. It is unclear as to what legal precedence that higher education has for noncompliance, since the majority of public universities and colleges receive a significant amount of governmental funding, whether it is at the federal or state level. It is also clear that government has not imposed any specific legal mandates per the Code of Federal Regulations, likely due to political repercussions, which may be summed-up in a word – lobbying. In an article for *Inside Higher Ed,* Doug Lederman explores lobbying and its influence on politics and higher education. Lederman reports,

> *"Higher education is a big business, and a lot of money is involved," says Celia Wexler, vice president for advocacy at Common Cause. "Lobbying has been a growth industry, a recession proof industry, and there is no indication we're going to see any less" in the future…. There are several reasons why lobbying spending would appear to be on the rise in higher education. (See Table 5) Wexler notes that the more heavily regulated an industry is, the more lobbying tends to increase, and the federal role in higher education has inarguably crept up in recent years….*

***Table 5. Reported Spent on Lobbying***

| Institution | 2005 Total | 2004 Total |
|---|---|---|
| University of Pittsburgh Medical Center | $1,406,000 | $980,000 |
| Johns Hopkins University | $1,020,000 | $620,000 |
| University of California System | $980,000 | $834,000 |
| American Council on Education | $640,000 | $160,000 |
| Northwestern University | $621,467 | $180,000 |

> *Some of the biggest names in Higher Ed lobbying spending, such as Johns Hopkins and Northwestern, tend to have significant long-term research relationships that they seek to nurture; Hopkins has engaged in several major projects with the National Aeronautics and Space Administration, for instance…. Most of the growth in recent years in higher education lobbying – particularly that done by individual colleges and universities – has been in hot pursuit of federal earmarks, known popularly by the less generous term of pork barrel projects. [***89***]*

A risk for universities, even those engaged heavily in lobbying, is that, if a level of compliance is not met, fiscal resources from the federal government will be unavailable for faculty research needs, based upon legal grant constraints requiring FISMA compliance.

Higher education is not opposed to effective standards for information and information systems security. Nevertheless, not being opposed to the standards does not signify support of FISMA's vision, mission, and embracing of the certification and accreditation process for their educational institution's information and information systems. It has been clearly stated that higher education leadership administrative staff hierarchy and structure does not support the current government and industry standards and practices administrative roles and associated responsibilities for CIO's and CISO's. These positions, roles, and responsibilities are critical to the effectiveness of information and information system security, although the hierarchy and

structure are slowly changing. There are other areas where structural changes would be required to make FISMA compliance effective for institutions where they simply may not have the available resources.

How the current FISMA implementation invites participation from its constituents to make it a more effective and practical process was identified. The role of education has always been to contribute and support the furtherance of technological development. Why would higher education not want to be more involved in directing the efforts of standardization for more security in information and information systems? The perception presented by many authors is that if the initiative is not directed, managed, and controlled by the "institution of higher education" then it must be suspect and self-serving.

Inevitably, the higher education systems security will be breached and cause irreparable harm to those who have entrusted their privileged information. With each breach would come the loss of public trust and the inevitable undermining of confidence in the higher educational system. Not only will confidence be lost, but also financial remuneration will be required to compensate for the negligence associated with the breach. Here, unquestionably the prosecuting attorney will cross-examine the defendant and accused (higher education) with a discourse regarding the level of due diligence of security for information and information systems. Is it possible they will bring up the issues of FISMA compliance? Quite possibly, yes, if the breach happened between a non-certified and accredited system of higher education and federally protected information and information system.

What options possibly exist for higher education's securing of key business processes involving information technology? Other than just embracing FISMA wholeheartedly, the first approach is the implementation of FISMA compliance as a "Do-it-yourself" approach. This type

of approach would likely take pieces of the FISMA model and manipulate them to manageable levels. At each level attained, another application of information or information system alignment would take place. Though this clearly is a strategy for long-term compliance alignment, until completion, graduated levels of risk will inevitably have to be accepted by the institution. Through this process, educational institutions will be held accountable for their decision making process when exploited due to negligence; however, having an actionable program in place does reduce liability. Another approach would be the outsourcing of information systems functionality, requirements, and more importantly liability. Two types of this method would be to completely outsource the solution, or collaborate with an external service provider for a hybrid implementation. Again, in the case of a hybrid method, a clear line of responsibility and liability would need to be identified.

Does the functional mission of the higher educational institution affect how the FISMA requirements should be applied? In other words, does the application of FISMA standards affect a research institution more than it influences a four-year or two-year university or college? Higher educational institutions normally create, secure, and portray for themselves and others as a separate subculture in society, which reflects a microcosm of what is found in the real world. This subculture includes shops, restaurants and other commerce, medical facilities, public safety, housing, theater and social events, etc., all within the confines of the institution's campus. Each institution of higher learning would have to determine the level of application per the functional disciplines they teach, and the operational requirements to support the faculty and students, as well as the administrative infrastructures they service and support. There is no one size fits all since the application of technology, and the compilation of information will differ from

institution to institution. What is even more complex is how FISMA will influence alumni associations or auxiliary services that have been sheltered under a non-profit educational status.

Attitudes in taking ownership of the FISMA requirements will vary from institution to institution. The response is unpredictable and will likely be based upon the style and preference of the institutional leadership – moreover their culture. One could expect at least three different approaches:

- Slow response or the "Tell me more after it has the bugs worked out" attitude – the typical response is to fight change or compliance;
- Medium response, or pack mentality maintainers – typically identified with most bureaucratic systems, that assume not all of the rules apply to them; or
- Fast or early adopters – the exception, some institutions may be proactive.

To place these responses in perspective, over two decades earlier in an article titled *Professional Codes of Conduct and Computer Ethics Education*, professors Martin and Martin demonstrated a clear lack of ownership regarding the "due diligence" challenge to higher education for information and information system accountability. From the Department of Electrical Engineering and Computer Science, from George Washington University, Martin and Martin identified to academia the need for a timely response, to what was particularized as an issue then. In this article they concluded,

> *Yet, our analysis of the professional codes of conduct reveals that they are inadequate to deal with emerging technological issues resulting from advancements in the computer field. There appears to be a lack of focus in the computer field in integrating ethical behavior into professional practice. While not wishing to be alarmists, we are suggesting that there needs to be a concerted effort on the part of the all the computer professional*

> *societies to update their ethical codes and to incorporate a process of continual self-assessment with formal procedures for the reporting of suspected improper practices, the availability of due process considerations, and the use of sanctions and possible disciplinary actions. [***90***]*

They continued and challenged higher education to be proactive in their ethical responsibility to curb the possible negative influence of public opinion and regulatory mandates and stated:

> *Because of the sensational media reporting of computer-related irregularities and because of the possible far-reaching consequences of computer abuse, the computer field is coming under increasing scrutiny at all levels of government. To prevent the government from imposing inflexible regulations that might retard computer research and development, the professional societies should take proactive measures toward self-regulation. [***90***]*

The aforementioned timelines and effort of higher education's response will vary depending upon the level of ownership the institution is willing to undergo, but will it require another two decades? If one compares the results from the earlier mentioned reports for the current government agencies FISMA compliance, the outlook will barely pass acceptable standards. Sadly, many higher educational institutions do not have the framework in place to support regulatory requirements, or similar changes, and therefore will require external motivation before precedence and priority of action can be taken. In all likelihood, the institutions will have to transition through a series of phases similar to most military decision-making processes such as the:

- Observation and understanding of requirements, whereby higher education will educate and convince themselves of FISMA's benefit. Since distrust from external influence of government influence is a commonly held attitude by many in academia, this will present a challenge;
- Orientation of individual institutional mission to FISMA requirements and what is justifiable as applicable to their goals or objectives. If FISMA is not recognized as bringing benefit to their operational and functional needs, and quantified in practical terms that signify financial gain or mitigation of financial loss, no ownership of the process will be undertaken;
- Decision making process that is effective and creates the necessary structure to support change – the institution must establish effective goals and objectives, with obtainable milestones that lead to FISMA compliance. Too often, this is where the process breaks down due to the bureaucratic political balance of power within academia. Someone, somehow, must address how compliance with FISMA will or will not impact "academic freedoms;" and
- Action upon the goals, objectives and milestones – project management, fiscal support, and utilization of all the physical and cultural resources higher education invests and maintains. This means that the process cannot be isolated to a few (see earlier comments), but must be embraced by all spheres of influence, whether administrative or relevant authority. These commonly recognized spheres are the technology department components (whether a part of the main service and support unit or specific to a school or department), administrative staff, auxiliary services, and faculty and students.

### *Higher Education's Challenge with FISMA Compliance*

As seen in earlier comments from various sources, the challenges higher education faces have already been self-identified. To narrow the scope of requirements one may need to apply levels of resolve that will be daunting and not well received. The first challenge higher education must address is what FISMA means to each institution and how to classify and divide information and information systems so the "academic freedom" mantra is not violated. The second challenge will be to determine how to gain ownership of an effective process that is not so costly that it impedes the institution's capability to perform their primary mission of educating our nation. The third and last challenge will be for higher education to measure effectively and consistently the results of compliance efforts for change, so that progress on security of information and information system for compliance can be demonstrated; despite the many breaches, they will inevitably experience. Higher education will have to promote and market FISMA compliance and its benefits, since there will always be "naysayers" who will want to scream from the mountain tops to undermine the efforts of what effective security should look like in practical terms.

From these challenges, the following set of guidelines should be given consideration in addressing the higher education's institutional requirements. The minimum framework and key components that must be in place to assimilate the FISMA requirements successfully are:

- System inventory: A comprehensive inventory of systems on the network and reconciliation of inventory to deployed security controls;
- Incident response: Incident response program for security of all information and information systems;

- Security monitoring: Automated monitoring of security events. Index audit trails across firewalls, applications, access control, IDS and any other component (this is a requirement in accordance with SCAP);
- Security reporting: Demonstrate compliance for all information protection controls, e.g., monitor, review and retain audit trails;
- Secure data retention: Secure capture and retention for all IT data for the times required by NIST standards; and
- Audit trail review: Routine NIST-mandated audit trail review.

This high-level guidance for a systematic process to assist educational institutions to prepare and implement FISMA regulatory requirements is available in many forms of technological application or appliances. Though technology and its security is the major focus, the most difficult step associated with the entire challenge is the people, and not the systems they use.

## 8. CONCLUSION

Much research, analysis, and considerations have gone into the compilation of what has been presented. The topic is vast, since its inception and institution in 2002; little has been published from the academic side regarding a response to federal regulatory requirements that seem to apply directly to its well-being. It is alarming that, over the past decade, the volume of information addressing higher education, federal regulations, compliance, liability and negligence, originating from within the halls of higher education, has sharply reduced in coverage and depth of scope. For example, the EDUCAUSE *2012 Strategic Plan*'s mention of federal compliance and more specifically FISMA was naught. [***91***] Why has academia not responded with didactic research and inquiry regarding this issue and many others that it faces? Has higher education taken a stance and class as "untouchable?" Alternatively, have they chosen to ignore the issue until the inevitable occurs? The likely reason is that higher education has not yet assumed ownership and responsibility (usually mandated through some compliance mechanism) or knows how to handle the responsibilities that they have been entrusted, and that it will take time before ownership of the process can take place.

Recall Rodney Peterson's article *Safeguarding Information Assets in Higher Education – The Role of the CSO*. Peterson concludes his discussion with,

> *Higher education institutions face issues of risk, liability, business continuity, cost, and national repercussions as they increasingly move their core activities to the Internet. College and Universities also play a unique role as the managers of some of the largest collections of computers on many of the fastest networks… The first key element for success is building a program around a solid system of information security governance (ISG). [***33***]*

Ownership is key to governance – a sign of a mature information security program. Ironically, it is often the excuse that compliance stifles openness and exchange of information. However, the very definition of information security is found within the tenants of confidentiality, integrity, and availability suggests otherwise. Again Peterson concludes, "The second key element for success is the development, implementation, and periodic review of a comprehensive IT, security plan." [***33***] Section 3542 of the *Federal Information Security Management Act* (H. R. 2458-49) states,

> *(1) The term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—*
>
> *(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information no repudiation and authenticity;*
>
> *(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and*
>
> *(C) availability, which means ensuring timely and reliable access to and use of information. [***13***]*

Where within the halls of higher learning is the definition of availability limiting? In addition, what good is research data if there is a question of its integrity or lack there of? Higher education likes its autonomy and strives to maintain its distinction from mainstream ideology, so that it can claim an unbiased position in society.

> *A common theme in higher education security literature has been the difficulty of the match between decentralized higher education culture and the culture of control needed for effective IT security…. A common critique of the higher education environment is its emphasis on decentralization and autonomy for academic units and faculty. [**1**]*

Unfortunately, there is more at stake than the role of self-proclaimed "academic freedoms."

> *Slammer*[37] *opened the door to a new view of IT security, a view that protecting academic networked resources in many cases trumped openness when it came to network design and architectures…. Concerns about confidentiality, integrity, and availability of data and the need to manage the risks of institutional embarrassment that comes from breaches have been cited as reasons for organizational leaders' choosing to invest in IT security programs…. It is abundantly clear that IT security is an institutional imperative, has critical policy and operational aspects, involves the engagement of important elements of institutions' leadership – CIO, general council, internal audit – and demands an increasingly knowledgeable and specialized professional workforce.* [***1***]

The security of information and information systems pose challenges of critical importance in our society today. In this day of communication, information is the most valuable commodity in existence. A mantra of higher education is "knowledge is power." To have knowledge of information regarding an individual implies that you have the ability to manipulate circumstances to that person's benefit or determent. To have knowledge of information regarding an individual also implies the potential for personal gain from its possession.

There are benefits that higher education can gain from FISMA and these benefits must be contextualized by each individual institution and evaluated to determine the level of benefit it

[37] Slammer was a worm that affected 75,000 hosts within 10 minutes of its release on January 25, 2008.

can bring to their organization's functionality. One must understand that, at a minimum, higher education's compliance to FISMA need only to include those systems accessing and or storing federally protected information or information systems. However, once the accreditation and certification process is understood and the cost of compliance is justified against the cost of breach, why not have all critical systems of an institution included and made compliant as well? FISMA offers standardizations that are peer-reviewed, which higher education could be key players in establishing. NIST has already invested billions of dollars in effort and in formalizing FISMA processes that are eclectic and flexible to any agency's needs. [***92***] FISMA addresses legal issues of due-diligence and places tested and validated safeguards in place for the security of information and information systems. What's more, private industry is involved in and utilizes FISMA standards, and shapes their business objectives to ensure compliance and accreditation. FISMA can support the academy's need for self-assessment and evaluation of its security program and external objectivity for functional business processes that exist in the various subcultures systems that support their infrastructure.

Are there challenges for higher education that may require other structural changes within their organization? Most certainly, with change comes a new perspective that will shape new ways of doing business for higher education. To aid in this, Peterson adds," The final key element for success is the establishment of appropriate benchmarks and metrics." [***33***] This metric may take form as governance (maturity) models. In an EDUCAUSE's Center for Applied Research paper titled *Progress and Politics: IT Governance in Higher Education*, authors Ronald Yanosky and Jack McCredie expound on the importance of metrics in the form of governance.

> *Governance must be shared among all major stakeholders, not just faculty, students, administrators, and trustees, on the basis of mutual respect and open communication…. Institutions… must find ways to "work patiently within identified collegial networks and eventually to fold multiple perspectives together while creating rolling visions of change." Higher education IT leaders will quickly note, however, that existing IT governance models are largely based on corporate practice, and that they may assume organizational hierarchies, or identify performance goals, that don't map directly to such higher education realities as shared governance, decentralized authority and funding, academic freedom, and nonprofit status. [***93***]*

However, these challenges faced by the academy's administration can be overcome through inclusivity and participation. Addressing this challenge Yanosky and McCredie state,

> *There is more to inclusivity than protecting your back; it also offers a way to share the burdens and responsibilities of IT leadership – in effect, to distribute them in ways that parallel the mix of interests inherent in a hybrid central/local/commodity IT environment. "Part of my goal." says James Hilton of his outreach efforts with faculty "is to move governance out of the community that sits back and critiques to a community that actually has a joint stake and joint accountability in this stuff." [***93***]*

Per Bill Readings in *The University in Ruins,* "It is no longer clear what role the University plays in society. The structure of the contemporary University is changing rapidly, and we have yet to understand precisely what these changes will mean." The university system must evolve to take on the responsibility they have already encumbered through use of federally protected information and information systems and apprehend a new determination of security

and stewardship for the overall environment. Given this future direction, higher education's next logical step to achieve recognizable security accreditation and certification may well be FISMA!

## 9. RESOURCES

[1] Gail Slaway, Mark Nelson, Rodney Peterson, Shannon Portillo Marilu Goodyear, "The Career of the IT Security Officer in Higher Education," EDUCAUSE Center for Applied Research, ECAR Occasional Paper 2006.

[2] Mohammad H Qayoumi and Carol Woody, "Addressing Information Security Risk," *EDUCAUSE Quarterly*, vol. 28, no. 4, pp. 7-11, September-December 2005.

[3] Kenneth D Salomon, Peter C Cassat, and Briana E Thibeau, "IT Security for Higher Education: a Legal Perspective," EDUCAUSE/Internet2 Computer and Network Security Task Force, Whitepaper ID: CSD2746, March 2003.

[4] Rodney Peterson and Jack Suess, "Briefing to CSIS Commission on Cyber Security for the 44th Presidency," EDUCAUSE/Internet2 Security Task Force, Brief ID: CSD5363, 2008.

[5] Christopher Jones. (2010) The Battle to Protect Sensitive Information on Government and Education Systems. [Online]. http://www.bytware.com/media/articles/protecting_government_information.html

[6] EDUCAUSE. (2002, July) Higher Education Contribution to National Stratagy to Secure Cyberspace. [Online]. http://net.educause.edu/ir/library/pdf/NET0027.pdf

[7] Triumfant. (2009, March) Federal Information Security Management Act (2002) Driving the Need for Automated Controls. [Online]. http://www.triumfant.com/pdfs/FISMA_Whitepaper_for_Triumfant.pdf

[8] Georgia.gov. (2008, March) Governor Perdue Signs Executive Order Strengthening State's Information Technology Security. [Online]. http://www.georgia.gov/00/press_print/0,2669,78006749_107734709_109366406,00.html

[9] Mark Reardon. (2008, April) Georgia Is On The Right Track With Security As Well. [Online]. http://www.georgia.gov/00/blog/detail/0,2775,1070969_117734979_112230769,00.html

[10] M. Peter Adler, "A Unified Approach to Information Security Compliance," *EDUCAUSE Review*, vol. 41, no. 5, pp. 46-61, September/October 2006.

[11] John Voloudakis, "The Continuing Evolution of Effective IT Security Practices," *EDUCAUSE Review*, vol. 41, no. 5, pp. 30-45, September/October 2006.

[12] National Institute of Standards and Technology - Computer Security Division, Computer Security Resource Center. (2012, February) Special Publications (800 Series). [Online]. http://csrc.nist.gov/publications/PubsSPs.html

[13] National Institute of Standards and Technology - Detailed Overview of FISMA (2002, October). (2010, August) Federal Information Security Management Act (2002). [Online]. http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

[14] EDUCAUSE. (2008, May) 2007 Federal Computer Security Report Card. [Online]. http://www.educause.edu/blog/rodney/2007FederalComputerSecurityRep/167017

[15] Tom Davis. (2008, May) Eighth Report Card on Computer Security. [Online]. http://www.coact.com/FISMA/FISMA_FY2007_reportcard.pdf

[16] FISMA Center. (2010) FISMA Resources. [Online]. https://www.fismacenter.com/

[17] Jeffery Zients, Vivek Kundra, and Howard A Schmidt. (2010, April) FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management. Memorandum for Heads of Executive Departments and Agencies.

[18] The White House: Office of Management and Budget. (2011, March) Fiscal Year 2010 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002. [Online]. http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/FY10_FISMA.pdf

[19] Elizabeth Montalbano, "Federal Agencies Still Lag On FISMA Compliance," *Information Week*, March 2012.

[20] James A. Lewis, "Cybersecurity Two Years Later," Center for Strategic & International Studies, Washington D.C., Report ISBN 978-0-89206-625-4, 2011.

[21] U.S. Department of Homeland Security. (2011, November) Blueprint for a Secure Cyber Future. [Online]. http://www.dhs.gov/files/publications/blueprint-for-a-secure-cyber-future.shtm

[22] Bill Readings, *University in Ruins*, 1st ed. Boston, United States: Harvard University Press, 1997.

[23] Lawrence White, "Which Legal Issues Will Keep Colleges Busy in the Year 2012?," *The Chronicle of Higher Education: The Chronicle Review*, vol. 51, no. 38, p. B1, May 2005.

[24] EDUCAUSE. (2012, February) Resources. [Online]. http://www.educause.edu/resources

[25] Briam Markham. (2008, February) Data Classification and Privacy: A Foundation for Compliance. [Online]. http://www.oit.umd.edu/Publications/Data_Classification_Presentation_022908.pdf

[26] Yale University: ITS Secure Computing. (2010, March) Yale University & FISMA (Federal Information Security MAnagement Act) Requirements. [Online].

http://www.yale.edu/its/secure-computing/data/compliance/fisma.html

[27] National Institute of Standards and Technology - Special Publication 800-53A. (2008, July) Guide for Assessing the Security Controls in Federal Information Systems. [Online]. http://csrc.nist.gov/publications/nistpubs/800-53A/SP800-53A-final-sz.pdf

[28] National Institute of Standards and Technology. (2010, June) Security Controls. [Online]. http://csrc.nist.gov/groups/SMA/fisma/controls.html

[29] National Institute of Standards and Technology. (2011, May) 2010 Computer Security Division Annual Report. [Online]. http://csrc.nist.gov/publications/nistir/ir7751/nistir-7751_2010-csd-annual-report.pdf

[30] EDUCAUSE. (2012, January) Uncommon Thinking in. Policy. [Online]. http://www.educause.edu/policy

[31] The American Council for Technology (ACT) - Industry Advisory Council (IAC), "Business Value of CFO-CIO Collaberation," The American Council for Technology (ACT) - Industry Advisory Council (IAC), Fairfax, Report Paper. [Online]. http://www.actgov.org/

[32] Kathy Bergsma, "Information Security Governance," EDUCAUSE and INTERNET2, White Paper 2011.

[33] Rodney Peterson, "Safeguarding the Assets in Higher Education – The Role of the CSO," *EDUCAUSE Review*, vol. 41, no. 5, pp. 73-82, September/October 2006.

[34] The White House: Office of Management and Budget. (1996, February) CIRCULAR NO. A-130. [Online]. http://www.whitehouse.gov/omb/circulars_a130

[35] National Institute of Standards and Technology - Computer Security Division, Computer Security Resource Center. (2010, June) Risk Management Framework (RMF) Overview. [Online]. http://csrc.nist.gov/groups/SMA/fisma/framework.html

[36] Acquisition.gov. (Pg.7.1-2, Section 7.103) Federal Acquisition Regulation (FAR). [Online]. https://www.acquisition.gov/far/index.html

[37] National Institute of Standards and Technology - Computer Security Division, Computer Security Resource Center. (2011, October) Risk Management Framework (RMF) - Frequently Asked Questions (FAQ's), Roles and Responsibilities & Quick Start Guides (QSG's). [Online]. http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/index.html

[38] National Institute of Standards and Technology - Special Publication 800-37. (2010, February) Guide for Applying the Risk. [Online]. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

[39] International Organization for Standardization. (2010, June) ISO/IEC 27000:2009. [Online]. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41933

[40] U.S. Department of Homeland Security. (2004, August) Homeland Security Presidential Directive 12: Policy for a Common Indentification Standard for Federal Employees and Contractors. [Online]. http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm#1

[41] Sharon S Dawes, Kristine L Bloniarz, Patricia D Fletcher, and Kristine L Kelly, "Some Assembly Required: Building a Digital Government for the 21st Century," Center for Technology in Government University at Albany / SUNY, Albany, White paper www.ctg.albany.edu, 1999.

[42] Verisign. (2005, January) FISMA: Making the Grade - An Introduction to the Federal Information Security Management Act. [Online]. http://www.verisign.com/static/030927.pdf

[43] G. Sadowsky, J. X. Dempsey, B. J. Mack, and A. Schwartz, "Information Technology Security Handbook," Global Information and Technologies Department: The International Bank for Reconstruction and Development, Washington D.C., Handbook InfoDev 30075, 2003.

[44] U.S. Government Accountabiliy Office (GAO), "Improving Oversight of Access to Federal Systems and Data by Contractors Can Reduce Risk," U.S. Government Accountability Office, Washington D.C., Report to Congressional Requesters GAO-05-362, 2005.

[45] Weiling Ke and Xiaodong Wang, "How Do Governments Matter to the Creation of Digital Economy," Association of Computing Machines, New York, Preceedings: 10th International Conference on Electronic Commerce ISBN: 978-1-60558-075-3, 2008.

[46] Andy Ju An Wang, "Information Security Models and Metrics," Association of Computing Machines, New York, Preceedings: 73rd Annual Southeast Regional Conference - Volume 2 ISBN: 1-59593-059-0, 2005.

[47] New World Encyclopedia. (2010, February) Academic Freedom. [Online]. http://www.newworldencyclopedia.org/entry/Academic_freedom

[48] Dian Schaffhauser, "Lawyers Indentify The Six Biggest Legal Issues Facing IT Today, And How CIOs Can Avoid a Run-In With The Law," *Campus Technology*, vol. Volume 25, no. 5, March 2012.

[49] Joseph E. Campana, "How Safe Are We in Our Schools?," J. Campana & Associates LLC, Madison, White Paper 2008.

[50] Adam Dodge. (2012, February) Educational Security Incidents (ESI). [Online].

http://www.adamdodge.com/esi/

[51] Corporate Information Security Working Group. (2005, January) Report of the Best Practices and Metrics Teams. [Online]. http://www.issa.org/Downloads/BPMetricsTeamReportFinal111704Rev11095.pdf

[52] National Institute of Standards and Technology. (2011, November) Information Security and Privacy Advisory Board (ISPAB). [Online]. http://csrc.nist.gov/groups/SMA/ispab/index.html

[53] Newswire Today. (2012, February) Elemental Announces New FISMA Security Policy Framework for Federal Government Organizations. Press Release: http://www.newswiretoday.com/news/6112/.

[54] Market Wire. (2007, Dec) Whistleblower Hotline Systems Provider Ethical Advocate Receives Industry-first FISMA Certification. News release: http://findarticles.com/p/articles/mi_pwwi/is_200712/ai_n21160941/.

[55] netForensics. (2011) Federal Information Security Management Act (FISMA) Compliance. [Online]. http://www.netforensics.com/compliance/fisma_compliance/

[56] Bruce Levinson, "Federal Cybersecurity Best Practices Study: Information Security Continuous Monitoring," Center for Regulatory Effectiveness, Washington, D.C., Study http://www.thecre.com/fisma, 2011.

[57] The American Council for Technology (ACT) - Industry Advisory Council (IAC), "Improving FISM Effictiveness and Efficiency Through the Security Content Automation Program (SCAP)," The American Council for Technology (ACT) - Industry Advisory Council (IAC), Fairfax, White Paper 2008. [Online]. http://www.actgov.gov

[58] EDUCAUSE. (2004, January) Federal Policy Issues. [Online]. http://net.educause.edu/ir/library/pdf/NET0201.pdf

[59] The White House: Office of Management and Budget. (2012, February) Implementation of the Government Paperwork Elimination Act. [Online]. http://www.whitehouse.gov/omb/fedreg_gpea2/

[60] U.S. Archives. (2012, February) Paperwork Reduction Act (44 U.S.C. 3501 et seq.). [Online]. http://www.archives.gov/federal-register/laws/paperwork-reduction/

[61] Betty K. Steele. (2009, March) Due Diligence on IT Security. [Online]. http://www.baselinemag.com/c/a/Security/Due-Diligence-on-IT-Security/

[62] Goldie Blumenstyk, "Colleges Could Be Liable for Hackers' Attacks, Insurance Expert Warns," *The Chronicle of Higher Learning - Archives*, July 2001.

[63] Chris Blask. (2011, May) Security and Due Diligence. [Online]. http://www.infosecisland.com/blogview/14031-Security-and-Due-Diligence.html?sms_ss=twitter&at_xt=4de3f5f6732e1dd6,0

[64] Andrea L. Foster, "Insecure and Unaware," *The Chronicle of Higher Learning - Technology*, vol. 50, no. 35, p. A33, May 2004.

[65] Florence Olsen, "The Growing Vulnerability of Campus Networks," *The Chronicle of Higher Learning - Technology*, p. A35, March 2002.

[66] Margaret L. O'Donnell and Craig W. Parker, "How Colleges Can Navigate the Thicket of Federal Regulations," *The Chronicle of Higher Learning - The Chronicle Review*, vol. 51, no. 38, p. B5, May 2005.

[67] Kelly Field, "Survey Reaffirms That Colleges Are Fed Up With Federal Regulation," *The Chronicle of Higher Learning - Government*, September 2011.

[68] Kathleen Curry Santora and William A. Kaplin, "Preventive Law: How Colleges Can Avoid Legal Problems," *The Chronicle of Higher Learning - The Chronicle Review*, vol. 49, no. 32, p. B20, April 2003.

[69] Anne M. Payton, "Data Security Breach: Seeking a Persription for Adequate Remedy," in *InfoSecCD '06 Proceedings of the 3rd Annual Conference on Information Security Curriculum Development*, New York, 2006.

[70] Victoria W. Romney and Gordon W. Romney, "Neglect of Information Privacy Instruction: A Case of Educational Malpractice," in *CITC5 '04 Preceedings of the 5th Conference on Information Technology Education*, New York, 2004.

[71] Andrea L. Foster, "Worried About Hackers? Buy Some Insurance," *The Chronicle of Higher Learning - Archive*, vol. 53, no. 8, p. A41, October 2006.

[72] Mary Helen Miller, "The Cost of Data Breaches is Rising, Study Finds," *The Chronicle of Higher Learning - Blogs*, January 2010.

[73] Brock Read, "Ohio U. Will Not Have to Pay for Computer-Security Breaches, a Judge Says," *The Chronicle of Higher Learning - Blog*, August 2007.

[74] Andrea L. Foster, "A 3rd Data Breach Prompts a Reorganization of Ohio U. Computer Services," *The Chronicle of Higher Learning - Archives*, May 2006.

[75] Doug Lederman. (2011, April) Chapel Hill, Researcher Settle Dispute on Computer Security. [Online]. http://www.insidehighered.com/

[76] Eric Ferreri. (2011, May) Breach Costly for Researcher, UNC-CH. [Online]. http://www.newsobserver.com/2011/05/09/1185493/breach-costly-for-researcher-unc.html

[77] Josh Kelelr. (2010, November) Former Student Sues U. of Hawaii over Data Breaches. [Online]. http://chronicle.com/

[78] CRN Stefanie Hoffman. (2010, October) University of Hawaii Data Breach Exposes 40,000 Student Records. [Online]. http://www.crn.com

[79] KFVE The Home Team. (2012, February) Judge Approves UH Data Breach Settlement. [Online]. http://www.k5thehometeam.com

[80] UHDataBreachLawsuit. (2012) University of Hawai'i Data Breach Settlement. [Online]. http://www.uhdatabreachlawsuit.com/

[81] Brian Robinson. (2011) Federal Computer Week - FISMA Compliance Falls Short of Adequate Security. [Online]. http://fcw.com/

[82] Daniel Pulliam. (2005, April) FISMA Tied to Funding. [Online]. http://www.cccure.org/

[83] Frank Washkuck Jr. (2007, September) Is FISMA Fixable? [Online]. http://www.scmagazine.com/

[84] Tom Davis and J R Reagan. (2010, October) Analysis: In Defense of FISMA. [Online]. http://www.nextgov.com/

[85] Marthie M. Lessing, "Best Practices Show The Way to Information Security Maturity," Council for Scientific and Industrial Research, University of Johannesburg, White Paper 2008.

[86] Software Engineering Institute - Carnegie Mellon. (2012) CMMI Levels. [Online]. http://www.sei.cmu.edu/cmmi/solutions/appraisals/levels.cfm

[87] National Institute of Standards and Technology. (2011, October) Security Maturity Levels. [Online]. http://csrc.nist.gov/groups/SMA/prisma/security_maturity_levels.html

[88] Stephane Hamel. (2009, September) Review of Maturity Models. [Online]. http://blog.immeria.net/2009/09/review-of-maturity-models.html

[89] Doug Lederman. (2006, December) Anti-Lobbying Fever? Not in Higher Ed. [Online]. http://www.insidehighered.com

[90] C. Dianne Martin and David H. Martin, "Professional Codes of Conduct and Computer Ethics Education," *SAGE Journals - Social Sience Computer Review*, vol. 8, no. 1, pp. 96-

108, April 1990.

[91] EDUCAUSE / Internet2 Higher Endeducation Information Security Council. (2012, January) HEISC 2012-13 Strategic Plan. [Online]. http://net.educause.edu/ir/library/pdf/sec1001.pdf

[92] NIST. (2010, February) Public and Business Affairs. [Online]. http://www.nist.gov/public_affairs/releases/budget_2011.cfm

[93] Ronald Yanosky and Jack McCredie, "Progress and Politics: IT Governance in Higher Education," *EDUCAUSE Center for Applied Research*, vol. Volume 5, 2008.