IT Compliance at NMSU
Laws & Regulations

Presented by

Carlos S. Lobato, CISA, CIA, CISSP

IT Compliance Officer

Information & Communication Technologies Department

Data Privacy Laws/Regs

- FERPA (Family Educational Rights and Privacy Act)
- HIPAA (Health Insurance Portability and Accountability Act)
- GLBA (Gramm-Leach-Bliley Act)
- RFR (Red Flags Rule) – From Federal Trade Commission
- FISMA (Federal Information Security Management Act)
- PCI DSS (Payment Card Industry Data Security Standard)
- Other – next page

Other laws to consider:

The Communications Assistance for Law Enforcement Act (CALEA)	CALEA's purpose is to enhance the ability of law enforcement and intelligence agencies to conduct electronic surveillance
Federal Privacy Act of 1974	The Privacy Act states in part: No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains....
Electronic Communications Privacy Act	From a rights perspective, the ECPA protects individuals' communications against government surveillance conducted without a court order, from third parties without legitimate authorization to access the messages, and from the carriers of the messages, such as Internet service providers. However it appears to provide little privacy protection to employees with respect to their communications as conducted on the equipment owned by their employer.
Computer Fraud and Abuse Act of 1986	The Computer Fraud and Abuse Act is a law passed by the United States Congress in 1986 intended to reduce "hacking" of computer systems. It was amended in 1994, 1996 and in 2001 by the USA PATRIOT Act. The USA PATRIOT Act increased the scope and penalties of this act.
The Computer Security Act of 1987	The Computer Security Law of 1987, Public Law No. 100-235 (H.R. 145), (Jan. 8, 1988), was passed by the United States Congress. It was passed to improve the security and privacy of sensitive information in Federal computer systems and to establish a minimum acceptable security practices for such systems. It requires the creation of computer security plans, and the appropriate training of system users or owners where the systems house sensitive information.
International Traffic in Arms Regulations (ITAR)	Government regulations that control the export and import of defense-related articles and services on the United States Munitions List (USML). These regulations implement the provisions of the Arms Export Control Act (AECA). Its goal is to safeguard U.S. national security.
Digital Millennium Copyright Act of 1998	Many people see unauthorized music downloading as harmless and don't fully understand its consequences. Illegal downloading presents a serious issue on college campuses and can be costly to the university administration in terms of resources, such as excessive use of bandwidth and time spent responding to infringement notices sent by the RIAA (Recording Industry Association of America). The RIAA is very active in enforcing DCMA for their clients. For more information on how the RIAA works with Universities, go to the FAQ's on the RIAA site.
U.S. Copyright Law, October 2007	Copyright protection is afforded to any work that is in a form that can be seen, reproduced, or otherwise communicated.
The Clery Act	Requires colleges and universities to keep and disclose information about crime on and near their respective campuses.
Higher Education Opportunity Act	Governs the administration of federal student aid programs.

FERPA – How to comply?

- Privacy Technical Assistance Center (PTAC) Checklists:
  - Data Governance Checklist (Dec 2011)
    - Responsibility, Policies & Procedures at a High Level
  - Data Security Checklist (Dec 2011)
    - Technical controls i.e. Strong Passwords, etc.
  - Data Breach Response (Sept 2012)
    - Responding to the breach (Policy, Plan & Procedures)
    - Notification to affected parties & U.S. Dept. of Ed

HIPAA – How to Comply?

- The DHHS Office for Civil Rights created a HIPAA comprehensive audit program/checklist
  - Available online
  - Covers Privacy Rule requirements
  - Covers Security Rule requirements
  - Covers requirements for the Data Breach Notification Rule

GLBA – How to Comply?

- The FTC created a Complying with the Safeguards Rule Checklist
  - How to Comply
  - Securing Information
  - Technical controls – Strong Passwords, etc.
- The FTC also created a How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act Checklist

RFR – How to Comply?

- The FTC created a Complying with the Red Flags Rule Checklist
  - Identify/inventory covered accounts (Accounts Receivables) – Recurring payments to pay-off debt
  - Identifying relevant red flags
  - Detecting red flags
  - Responding to red flags
  - Administering your Program – Designate Responsibility, Policy, etc.
- The FTC also created a website with tips on How to Fight Fraud with the Red Flags Rule

FISMA - How to Comply?

- Applies to Universities via Federal Grants/Contracts
- FISMA Compliance Checklist/Overview, which requires the implementation of the various IT NIST Standards and Guidelines (National Institute of Standards and Technology)

PCI DSS – How to Comply?

- The PCI Security Standards Council created a Requirements and Security Assessment Procedures Checklist
- Additionally they created a section on their website that details "How to Be Compliant"

Main Requirements(FERPA, HIPAA, GLBA, RFR, FISMA and PCI)

- Designate Information Security Responsibility
- Establish a Risk-based Information Security Program
- Establish Policies & Procedures
- Monitoring/Incident Handling/Compliance
- Establish Training and Awareness

Why Comply ? ? ?

- **Is the law and we cannot look the other way**
- Remember – The protection & privacy of UNIVERSITY DATA (student, faculty & staff) is in our hands.
- It is EVERYONES responsibility & duty to safeguard this data.

Q & A

Carlos S. Lobato, CISA, CIA, CISSP

IT Compliance Officer

NMSU ICT – IT Compliance Function

clobato@nmsu.edu

http://compliance.ict.nmsu.edu/

646-5902

Thank you for your time!